PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-176191

(43)Date of publication of application : 29.06.2001

(51)Int.Cl. G11B 20/10
G11B 20/12
H04N 5/85
H04N 5/91
H04N 5/92

(21)Application number : 11-359398 (71)Applicant : SONY CORP

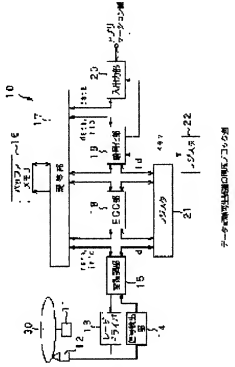
(22)Date of filing : 17.12.1999 (72)Inventor : CHIAKI SUSUMU

(54) DATA RECORDING/REPRODUCING METHOD AND DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To make difficult the decoding and the disk copy of the data recorded on a disk like recording medium.

SOLUTION: A data recording/reproducing device 10 is provided with a data processing means having at least an encode part 19 coding the data to be recorded on the disk like recording medium 30 and decoding the data to be reproduced recorded on the disk like recording medium 30. The encode part 19 records a disk ID peculiar to the disk like recording medium 30 during a frame synchronizing signal in the control area of the disk like recording medium 30 when the disk like recording medium 30 is initialized, and encodes the user data with the disk ID when the user data are recorded on the disk like recording medium 30.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－176191
（P2001－176191A）
(43)公開日　平成13年６月29日(2001.6.29)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ１１Ｂ 20/10		Ｇ１１Ｂ 20/10		Ｈ ５Ｃ０５２
20/12		20/12		５Ｃ０５３
Ｈ０４Ｎ 5/85		Ｈ０４Ｎ 5/85		Ｚ ５Ｄ０４４
5/91		5/91		Ｐ
5/92		5/92		Ｈ

審査請求　未請求　請求項の数62　ＯＬ　（全 36 頁）

(21)出願番号　特願平11－359398

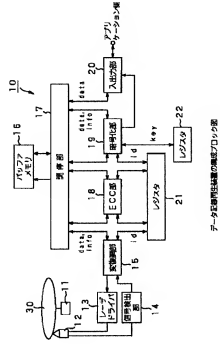
(22)出願日　平成11年12月17日(1999.12.17)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　千秋　進
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100067736
弁理士　小池　晃　（外２名）

Ｆターム(参考)　5C052 AA02 AB03 AB05 CC01 DD10
5C053 FA15 FA24 GB01 GB06 JA21
5D044 AB05 AB07 BC06 CC04 DE02
DE03 DE37 DE49 DE52 GK11
GK17

(54)【発明の名称】　データ記録再生方法及びデータ記録再生装置

(57)【要約】
【課題】　ディスク状記録媒体に記録されているデータの解読やディスクコピーを困難とする。
【解決手段】　データ記録再生装置１０は、ディスク状記録媒体３０に対して記録すべきデータを暗号化するとともに、ディスク状記録媒体３０に記録されている再生すべきデータを復号化する暗号化部１９を少なくとも有してデータ処理を行うデータ処理手段を備える。暗号化部１９は、ディスク状記録媒体３０の初期化時に、ディスク状記録媒体３０に固有のディスクＩＤディスク状記録媒体３０のコントロール領域におけるフレーム同期信号中に記録し、ディスク状記録媒体３０に対するユーザデータの記録時に、ディスクＩＤを用いてユーザデータを暗号化する。



1

【特許請求の範囲】

【請求項１】　ディスク状記録媒体に対するブロック単位でのデータの記録及び／又は再生を行うデータ記録再生方法であって、

上記ディスク状記録媒体の初期化時に、上記ディスク状記録媒体に固有の記録媒体識別情報を上記ディスク状記録媒体のコントロール領域における所定領域に記録し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報を用いて上記ユーザデータを暗号化することを特徴とするデータ記録再生方法。

【請求項２】　上記所定領域は、データを記録するためのデータ記録領域以外の領域であることを特徴とする請求項１記載のデータ記録再生方法。

【請求項３】　上記所定領域は、フレーム同期信号を記録するためのフレーム同期信号記録領域であることを特徴とする請求項２記載のデータ記録再生方法。

【請求項４】　上記ディスク状記録媒体の初期化時に、ランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、

上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を、上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、

上記記録媒体識別情報と上記記録媒体情報とを用いて記録媒体鍵情報を生成し、

上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項１記載のデータ記録再生方法。

【請求項５】　上記ディスク状記録媒体に対するユーザデータの記録時に、

上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記記録媒体鍵情報を生成し、

上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を、ユーザ領域における上記付加情報記録領域に記録し、

上記記録媒体鍵情報と上記ブロック情報とを用いてブロック鍵情報を生成し、

上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項４記載のデータ記録再生方法。

【請求項６】　上記ディスク状記録媒体に記録されているユーザデータの再生時に、

上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記記録媒体鍵情報を生成し、

上記ユーザ領域を再生して上記ブロック情報を取り出して、上記記録媒体鍵情報と上記ブロック情報とを用いて上記ブロック鍵情報を生成し、

2

上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項５記載のデータ記録再生方法。

【請求項７】　上記ディスク状記録媒体に対するユーザデータの記録時に、

上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記記録媒体鍵情報を生成し、

ランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、

上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を、上記ユーザ領域における上記付加情報記録領域に記録し、

上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報とを用いてブロック鍵情報を生成し、

上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項４記載のデータ記録再生方法。

【請求項８】　上記ディスク状記録媒体に記録されているユーザデータの再生時に、

上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記記録媒体鍵情報を生成し、

上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報とを取り出して、上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報とを用いて上記ブロック鍵情報を生成し、

上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項７記載のデータ記録再生方法。

【請求項９】　上記ディスク状記録媒体の初期化時に、ランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、

上記記録媒体識別情報と、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報とを用いて記録媒体鍵情報を生成し、

上記記録媒体鍵情報と、上記記録媒体情報として上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、

上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項１記載のデータ記録再生方法。

【請求項１０】　上記ディスク状記録媒体に対するユーザデータの記録時に、
上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、
ランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、
上記記録媒体鍵情報と、上記ブロック識別情報と、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報とを用いてブロック鍵情報を生成し、
上記ブロック鍵情報を、上記ブロック情報として上記ユーザ領域における上記付加情報記録領域に記録し、
上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項９記載のデータ記録再生方法。
【請求項１１】　上記ディスク状記録媒体に記録されているユーザデータの再生時、
上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、
上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報とを取り出して、上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報とを用いて上記ブロック鍵情報を生成し、
上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項１０記載のデータ記録再生方法。
【請求項１２】　上記ディスク状記録媒体の初期化時に、
ランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、
上記記録媒体識別情報を用いて、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報を暗号化して、記録媒体情報を生成し、
上記記録媒体情報を上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、
上記記録媒体情報を記録媒体鍵情報とし、
上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項１記載のデータ記録再生方法。
【請求項１３】　上記ディスク状記録媒体に対するユーザデータの記録時に、
上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

ランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、
上記記録媒体鍵情報と上記ブロック識別情報とを用いて、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報を暗号化して、ブロック情報を生成し、
上記ブロック情報を上記ユーザ領域における上記付加情報記録領域に記録し、
上記ブロック情報をブロック鍵情報とし、
上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項１２記載のデータ記録再生方法。
【請求項１４】　上記ディスク状記録媒体に記録されているユーザデータの再生時に、
上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、
上記ユーザ領域を再生して上記ブロック情報を取り出して、上記記録媒体鍵情報と上記ブロック情報とを用いて上記ブロック鍵情報を生成し、
上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項１３記載のデータ記録再生方法。
【請求項１５】　上記ディスク状記録媒体の初期化時に、
ランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、
上記ランダムデータを分割し、
上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報を暗号化して、記録媒体情報を生成し、
上記記録媒体情報を上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、
上記ランダムデータを分割して得られた他方のランダムデータと上記記録媒体情報とを用いて記録媒体鍵情報を生成し、
上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項１記載のデータ記録再生方法。
【請求項１６】　上記ディスク状記録媒体に対するユーザデータの記録時に、
上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記記録媒体鍵情報を生成し、

ランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、

上記ランダムデータを分割し、

上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報を暗号化して、ブロック情報を生成し、

上記ブロック情報を上記ユーザ領域における上記付加情報記録領域に記録し、

上記ランダムデータを分割して得られた他方のランダムデータと上記ブロック情報と上記記録媒体鍵情報とを用いてブロック鍵情報生成し、

上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項１５記載のデータ記録再生方法。

【請求項１７】　上記ディスク状記録媒体に記録されているユーザデータの再生時に、

上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記記録媒体鍵情報を生成し、

上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報とを取り出して、上記ブロック識別情報と上記ブロック情報と上記記録媒体鍵情報とを用いて上記ブロック鍵情報を生成し、

上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項１６記載のデータ記録再生方法。

【請求項１８】　上記ディスク状記録媒体の初期化時に、

ランダムデータを発生し、このランダムデータを物理ブロック番号を用いて暗号化して、上記ディスク状記録媒体における各ブロック毎に固有の上記記録媒体識別情報を生成し、

上記ランダムデータを分割し、

上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報を暗号化して、記録媒体情報を生成し、

上記記録媒体情報を上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、

上記ランダムデータを分割して得られた他方のランダムデータと上記記録媒体情報とを用いて記録媒体鍵情報を生成し、

上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項１記載のデータ記録再生方法。

【請求項１９】　上記ディスク状記録媒体に対するユーザデータの記録時に、

上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記記録媒体鍵情報を生成し、

ランダムデータを発生し、このランダムデータを上記物理ブロック番号を用いて暗号化して、上記各ブロック毎に固有のブロック識別情報を生成し、

上記ブロック識別情報を上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、

上記ランダムデータを分割し、

上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報を暗号化して、ブロック情報を生成し、

上記ブロック情報を上記ユーザ領域における上記付加情報記録領域に記録し、

上記ランダムデータを分割して得られた他方のランダムデータと上記ブロック情報と上記記録媒体鍵情報とを用いてブロック鍵情報生成し、

上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項１８記載のデータ記録再生方法。

【請求項２０】　上記ディスク状記録媒体に記録されているユーザデータの再生時に、

上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記記録媒体鍵情報を生成し、

上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報とを取り出して、上記ブロック識別情報と上記ブロック情報と上記記録媒体鍵情報とを用いて上記ブロック鍵情報を生成し、

上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項１９記載のデータ記録再生方法。

【請求項２１】　上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていることを示していた場合には、

復号化して出力すべき旨のコマンドを受けた場合にのみ、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力し、

復号化しないで出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力しないことを特徴とする請求項６記載のデータ記録再生方法。

【請求項２２】　上記ディスク状記録媒体に記録されて

いる制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていないことを示していた場合には、
復号化して出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力せず、
復号化しないで出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力することを特徴とする請求項２１記載のデータ記録再生方法。

【請求項２３】　上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報若しくは上記ブロック識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていることを示していた場合には、
復号化して出力すべき旨の正しいコマンドを受けた場合にのみ、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力し、
復号化しないでそのまま出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力しないことを特徴とする請求項８記載のデータ記録再生方法。

【請求項２４】　上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報若しくは上記ブロック識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていないことを示していた場合には、
復号化して出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力せず、
復号化しないで出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力することを特徴とする請求項２３記載のデータ記録再生方法。

【請求項２５】　上記ディスク状記録媒体の初期化時に、
ランダムデータを発生し、このランダムデータを上記記録媒体識別情報とし、この記録媒体識別情報を上記コントロール領域における上記所定領域としての付加情報を記録するための付加情報記録領域に記録し、
上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を上記コントロール領域における上記付加情報記録領域に記録し、
上記記録媒体識別情報と上記記録媒体情報とを用いて記録媒体鍵情報を生成し、
上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項１記載のデータ記録再生方法。

【請求項２６】　上記ディスク状記録媒体の初期化時に、
ランダムデータを発生し、このランダムデータを上記記録媒体識別情報とし、
上記記録媒体識別情報と、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報とを用いて記録媒体鍵情報を生成し、
上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データとともに、上記記録媒体識別情報と上記記録媒体情報とを、上記記録媒体識別情報を上記コントロール領域における上記所定領域としてのデータ記録領域に記録することを特徴とする請求項１記載のデータ記録再生方法。

【請求項２７】　上記ディスク状記録媒体に対するユーザデータの記録時に、
上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記記録媒体鍵情報を生成し、
ランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報とし、このブロック識別情報をユーザ領域における付加情報を記録するための付加情報記録領域に記録し、
上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を、上記ユーザ領域における上記付加情報記録領域に記録し、
上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報とを用いてブロック鍵情報を生成し、
上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項２５記載のデータ記録再生方法。

【請求項２８】　上記ディスク状記録媒体に対するユーザデータの記録時に、
上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記記録媒体鍵情報を生成し、
ランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報とし、
上記記録媒体鍵情報と、上記ブロック識別情報と、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時

情報の全部又は一部の情報であるブロック情報とを用いてブロック鍵情報を生成し、

上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータとともに、上記ブロック識別情報と上記ブロック情報とを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項２６記載のデータ記録再生方法。

【請求項２９】　上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報及び／又は上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を予め記憶していることを特徴とする請求項１記載のデータ記録再生方法。

【請求項３０】　ディスク状記録媒体に対するブロック単位でのデータの記録及び／又は再生を行うデータ記録再生装置であって、

上記ディスク状記録媒体に対して記録すべきデータを暗号化するとともに、上記ディスク状記録媒体に記録されている再生すべきデータを復号化する暗号化手段を少なくとも有してデータ処理を行うデータ処理手段を備え、

上記暗号化手段は、

上記ディスク状記録媒体の初期化時に、上記ディスク状記録媒体に固有の記録媒体識別情報を上記ディスク状記録媒体のコントロール領域における所定領域に記録し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報を用いて上記ユーザデータを暗号化することを特徴とするデータ記録再生装置。

【請求項３１】　上記所定領域は、データを記録するためのデータ記録領域以外の領域であることを特徴とする請求項３０記載のデータ記録再生装置。

【請求項３２】　上記所定領域は、フレーム同期信号を記録するためのフレーム同期信号記録領域であることを特徴とする請求項３１記載のデータ記録再生装置。

【請求項３３】　上記暗号化手段は、

ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、

鍵情報を生成するコントロール領域用鍵情報生成手段と、

暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体の初期化時に、上記コントロール領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を、上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、上記コントロール領域用鍵情報生成手段により上記記録媒体識別情報と上記記録媒体情報とを用いて記録媒体鍵情報を生成し、上記コントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項３０記載のデータ記録再生装置。

【請求項３４】　上記暗号化手段は、

鍵情報を生成するユーザ領域用鍵情報生成手段と、

暗号化及び／又は復号化を行うユーザ領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を、ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用鍵情報生成手段により上記記録媒体鍵情報と上記ブロック情報とを用いてブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項３３記載のデータ記録再生装置。

【請求項３５】　上記暗号化手段は、上記ディスク状記録媒体に記録されているユーザデータの再生時に、上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域を再生して上記ブロック情報を取り出して、上記ユーザ領域用鍵情報生成手段により上記記録媒体鍵情報と上記ブロック情報とを用いて上記ブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項３４記載のデータ記録再生装置。

【請求項３６】　上記暗号化手段は、

ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、

鍵情報を生成するユーザ領域用鍵情報生成手段と、

暗号化及び／又は復号化を行うユーザ領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域用ランダムデータ発生手段によりランダムデータを発生

し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を、上記ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用鍵情報生成手段により上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報とを用いてブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項３３記載のデータ記録再生装置。

【請求項３７】　上記暗号化手段は、上記ディスク状記録媒体に記録されているユーザデータの再生時に、上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報とを取り出して、上記ユーザ領域用鍵情報生成手段により上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報とを用いて上記ブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項３６記載のデータ記録再生装置。

【請求項３８】　上記暗号化手段は、

ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、

鍵情報を生成するコントロール領域用鍵情報生成手段と、

暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体の初期化時に、上記コントロール領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、上記コントロール領域用鍵情報生成手段によって、上記記録媒体識別情報と、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報である記録媒体情報とを再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記記録媒体情報を、上記記録媒体情報として上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、上記コントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項３０記載のデータ記録再生装置。

【請求項３９】　上記暗号化手段は、

ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、

鍵情報を生成するユーザ領域用鍵情報生成手段と、

暗号化及び／又は復号化を行うユーザ領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、上記ユーザ領域用鍵情報生成手段によって、上記記録媒体鍵情報と、上記ブロック識別情報と、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報とを用いてブロック鍵情報を生成し、上記ブロック鍵情報を、上記ブロック情報として上記ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項３８記載のデータ記録再生装置。

【請求項４０】　上記暗号化手段は、上記ディスク状記録媒体に記録されているユーザデータの再生時に、上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報とを取り出して、上記ユーザ領域用鍵情報生成手段により上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報とを用いて上記ブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項３９記載のデータ記録再生装置。

【請求項４１】　上記暗号化手段は、

ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、

鍵情報を生成するコントロール領域用鍵情報生成手段と、

暗号化及び／又は復号化を行う第１及び第２のコントロール領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体の初期化時に、上記コントロール領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記記録媒体識別情報

として上記コントロール領域における上記所定領域に記録し、上記第１のコントロール領域用暗号化及び／又は復号化手段によって、上記記録媒体識別情報を用いて、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報を暗号化して、記録媒体情報を生成し、上記記録媒体情報を上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、上記コントロール領域用鍵情報生成手段により上記記録媒体情報を記録媒体鍵情報とし、上記第２のコントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項３０記載のデータ記録再生装置。

【請求項４２】　上記暗号化手段は、

ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、

鍵情報を生成するユーザ領域用鍵情報生成手段と、

暗号化及び／又は復号化を行う第１及び第２のユーザ領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、上記第１のユーザ領域用暗号化及び／又は復号化手段によって、上記記録媒体鍵情報と上記ブロック識別情報とを用いて、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報を暗号化して、ブロック情報を生成し、上記ブロック情報を上記ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用鍵情報生成手段により上記ブロック情報をブロック鍵情報とし、上記第２のユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項４１記載のデータ記録再生装置。

【請求項４３】　上記暗号化手段は、上記ディスク状記録媒体に記録されているユーザデータの再生時に、上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域を再生して上記ブロック情報を取り出して、上記ユーザ領域用鍵情報生成手段により上記記録媒体鍵情報と上記ブロック情報とを用いて上記ブロック鍵情報を生成し、上記第２のユーザ領域用暗号化及び／又は復号化手段により上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項４２記載のデータ記録再生装置。

【請求項４４】　上記暗号化手段は、

ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、

鍵情報を分割するコントロール領域用鍵情報分割手段と、

鍵情報を生成するコントロール領域用鍵情報生成手段と、

暗号化及び／又は復号化を行う第１及び第２のコントロール領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体の初期化時に、上記コントロール領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、上記コントロール領域用鍵情報分割手段により上記ランダムデータを分割し、上記第１のコントロール領域用暗号化及び／又は復号化手段によって、上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報を暗号化して、記録媒体情報を生成し、上記記録媒体情報を上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、上記コントロール領域用鍵情報生成手段により上記ランダムデータを分割して得られた他方のランダムデータと上記記録媒体情報とを用いて記録媒体鍵情報を生成し、上記第２のコントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項３０記載のデータ記録再生装置。

【請求項４５】　上記暗号化手段は、

ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、

鍵情報を分割するユーザ領域用鍵情報分割手段と、

鍵情報を生成するユーザ領域用鍵情報生成手段と、

暗号化及び／又は復号化を行う第１及び第２のユーザ領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、上記ユーザ領域用鍵情報分割手段により上記ラン

ダムデータを分割し、上記第１のユーザ領域用暗号化及び／又は復号化手段によって、上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報を暗号化して、ブロック情報を生成し、上記ブロック情報を上記ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用鍵情報生成手段により上記ランダムデータを分割して得られた他方のランダムデータと上記記録媒体鍵情報とを用いてブロック鍵情報生成し、上記第２のユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項４４記載のデータ記録再生装置。

【請求項４６】　上記暗号化手段は、上記ディスク状記録媒体に記録されているユーザデータの再生時に、上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報とを取り出して、上記ユーザ領域用鍵情報生成手段により上記ブロック識別情報と上記ブロック情報と上記記録媒体鍵情報とを用いて上記ブロック鍵情報を生成し、上記第２のユーザ領域用暗号化及び／又は復号化手段により上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項４５記載のデータ記録再生装置。

【請求項４７】　上記暗号化手段は、

ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、

鍵情報を分割するコントロール領域用鍵情報分割手段と、

鍵情報を生成するコントロール領域用鍵情報生成手段と、

暗号化及び／又は復号化を行う第１、第２及び第３のコントロール領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体の初期化時に、上記コントロール領域用ランダムデータ発生手段によりランダムデータを発生し、上記第１のコントロール領域用暗号化及び／又は復号化手段によりこのランダムデータを物理ブロック番号を用いて暗号化して、上記ディスク状記録媒体における各ブロック毎に固有の上記記録媒体識別情報を生成し、上記コントロール領域用鍵情報分割手段により上記ランダムデータを分割し、上記第２のコントロール領域用暗号化及び／又は復号化手段によって、上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報を暗号化して、記録媒体情報を生成し、上記記録媒体情報を上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、上記コントロール領域用鍵情報生成手段により上記ランダムデータを分割して得られた他方のランダムデータと上記記録媒体情報とを用いて記録媒体鍵情報を生成し、上記第３のコントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項３０記載のデータ記録再生装置。

【請求項４８】　上記暗号化手段は、

ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、

鍵情報を分割するユーザ領域用鍵情報分割手段と、

鍵情報を生成するユーザ領域用鍵情報生成手段と、

暗号化及び／又は復号化を行う第１、第２及び第３のユーザ領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、ユーザ領域用ランダムデータ発生手段によりランダムデータを発生し、上記第１のユーザ領域用暗号化及び／又は復号化手段によりこのランダムデータを上記物理ブロック番号を用いて暗号化して、上記各ブロック毎に固有のブロック識別情報を生成し、上記ブロック識別情報を上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、上記ユーザ領域用鍵情報分割手段により上記ランダムデータを分割し、上記第２のユーザ領域用暗号化及び／又は復号化手段によって、上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報を暗号化して、ブロック情報を生成し、上記ブロック情報を上記ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用鍵情報生成手段により上記ランダムデータを分割して得られた他方のランダムデータと上記記録媒体鍵情報とを用いてブロック鍵情報生成し、上記第３のユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項４７記載のデータ記録再生装置。

【請求項４９】　上記暗号化手段は、上記ディスク状記録媒体に記録されているユーザデータの再生時に、上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記コントロール領域用鍵情報生成手段により

上記記録媒体鍵情報を生成し、上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報とを取り出して、上記ユーザ領域用鍵情報生成手段により上記ブロック識別情報と上記ブロック情報と上記記録媒体鍵情報とを用いて上記ブロック鍵情報を生成し、上記第３のユーザ領域用暗号化及び／又は復号化手段により上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項４８記載のデータ記録再生装置。

【請求項５０】　上記暗号化手段は、上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていることを示していた場合には、復号化して出力すべき旨のコマンドを受けた場合にのみ、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力し、復号化しないで出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力しないことを特徴とする請求項３５記載のデータ記録再生装置。

【請求項５１】　上記暗号化手段は、上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていないことを示していた場合には、復号化して出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力せず、復号化しないで出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力することを特徴とする請求項５０記載のデータ記録再生装置。

【請求項５２】　上記暗号化手段は、上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報若しくは上記ブロック識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていることを示していた場合には、復号化して出力すべき旨の正しいコマンドを受けた場合にのみ、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力し、復号化しないでそのまま出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力しないことを特徴とする請求項３７記載のデータ記録再生装置。

【請求項５３】　上記暗号化手段は、上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報若しくは上記ブロック識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていないことを示していた場合には、復号化して出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力せず、復号化しないで出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力することを特徴とする請求項５２記載のデータ記録再生装置。

【請求項５４】　上記データ処理手段は、上記データ処理を行うためにデータを一時記憶する一時記憶手段を有することを特徴とする請求項３０記載のデータ記録再生装置。

【請求項５５】　上記データ処理手段は、上記ディスク状記録媒体に対してレーザ光を照射するとともにその戻り光を受光する光学ピックアップ手段から出力された信号を電流－電圧変換して得られた信号からデータを検出する信号検出手段を有することを特徴とする請求項５４記載のデータ記録再生装置。

【請求項５６】　上記データ処理手段は、データの変調及び／又は復調を行う変復調手段と、データに対する誤り訂正及び／又は誤り検出を行う誤り訂正及び／又は誤り検出手段と、外部とのデータの入出力を行うための入出力手段と、データに対する暗号化及び復号化に必要となる情報を保持する記憶手段と、上記変復調手段、上記誤り訂正及び／又は誤り検出手段、上記暗号化手段又は上記入出力手段と上記データ処理を行うためにデータを一時記憶する一時記憶手段との間で行われるデータの入出力を調停する調停手段とを少なくとも有することを特徴とする請求項３０記載のデータ記録再生装置。

【請求項５７】　上記暗号化手段は、

ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、

鍵情報を生成するコントロール領域用鍵情報生成手段と、

暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体の初期化時に、コントロール領域用ランダムデータ発生手段によりランダムデータを発生させ、このランダムデータを上記記録媒体識別情報とし、この記録媒体識別情報を上記コントロール領域における上記所定領域としての付加情報を記録するための付加情報記録領域に記録し、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を上記コントロール領域における上記付加情報記録領域に記録し、上記コントロール領域用鍵情報生成手段により上記記録媒体識別情報と上記記録媒体情報とを用いて記録媒体鍵情報を生成し、上記コントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報

を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項５４記載のデータ記録再生装置。

【請求項５８】　上記暗号化手段は、

ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、

鍵情報を生成するコントロール領域用鍵情報生成手段と、

暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体の初期化時に、上記コントロール領域用ランダムデータ発生手段によりランダムデータを発生させ、このランダムデータを上記記録媒体識別情報とし、上記コントロール領域用鍵情報生成手段によって、上記記録媒体識別情報と、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報とを用いて記録媒体鍵情報を生成し、上記コントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データとともに、上記記録媒体識別情報と上記記録媒体情報とを、上記コントロール領域における上記所定領域としてのデータ記録領域に記録することを特徴とする請求項５４記載のデータ記録再生装置。

【請求項５９】　上記暗号化手段は、

ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、

鍵情報を生成するユーザ領域用鍵情報生成手段と、

暗号化及び／又は復号化を行うユーザ領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報とし、このブロック識別情報をユーザ領域における付加情報を記録するための付加情報記録領域に記録し、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を、上記ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用鍵情報生成手段により上記記録媒体識別情報と上記ブロック識別情報と上記ブロック情報とを用いてブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項５７記載のデータ記録再生装置。

【請求項６０】　上記暗号化手段は、

ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、

鍵情報を生成するユーザ領域用鍵情報生成手段と、

暗号化及び／又は復号化を行うユーザ領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報とし、上記ユーザ領域用鍵情報生成手段によって、上記記録媒体鍵情報と、上記ブロック識別情報と、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報とを用いてブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータとともに、上記ブロック識別情報と上記ブロック情報とを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項５７記載のデータ記録再生装置。

【請求項６１】　上記暗号化手段は、情報を記憶する記憶手段を有し、

上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報及び／又は上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を上記記憶手段に予め記憶していることを特徴とする請求項３０記載のデータ記録再生装置。

【請求項６２】　上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報及び／又は上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を上記一時記憶手段に予め記憶していることを特徴とする請求項５４記載のデータ記録再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディスク状記録媒体に対するデータの記録及び／又は再生を行うデータ記録再生方法及びデータ記録再生装置に関する。

【０００２】

【従来の技術】例えば高画質のディジタルビデオ信号等

のディジタルデータを光学的に記録したディスク状記録媒体として、再生専用であるＤＶＤ（Digital Versatile Disc又は Digital Video Disc）が広く知られている。また最近では、このＤＶＤフォーマットを用いて、追記や書き換えを可能としたディスク状記録媒体として、ＤＶＤ－Ｒ（DVD-Recordable）、ＤＶＤ－ＲＷ（DVD-ReWritable）、ＤＶＤ－ＲＡＭ（DVD-Random Access Memory）の商品化や開発が進められている。

【０００３】このようなディスク状記録媒体においては、ユーザデータ、制御情報及びＩＤ情報等が１つのブロックとして誤り訂正符号化され、この誤り訂正符号化されたデータが変調され、さらに同期信号が付加されて記録される。

【０００４】例えばＤＶＤのフォーマットは、図１６に示すように、ユーザデータ、制御情報及びＩＤ情報等からなる１７２バイト×１９２バイト＝３３０２４バイトのＥＣＣ（Error Correcting Code）ブロックに対して同図中斜線部に示すパリティが付加されたいわゆる積符号の構成となる。ＤＶＤにおいては、誤り訂正符号としてＲＳ（Read Solomon Code）が用いられる。ＤＶＤにおいては、行方向をＣ１、列方向をＣ２とすると、Ｃ１は、ＲＳ（１８２，１７２，１１）、Ｃ２は、ＲＳ（２０８，１９２，１７）である。

【０００５】この１ブロック分のデータは、ディスク状記録媒体上の１６セクタ分に相当する。ディスク状記録媒体の１セクタは、２６フレームから構成され、１フレームは、９１バイトのデータから構成される。また、各フレームには、フレーム同期信号が付加される。すなわち、ディスク状記録媒体上に並べられるパリティ以外のデータは、図１７に示すように、９１バイト×４１６フレーム（１６セクタ×２６フレーム）から構成される。

【０００６】ディスク状記録媒体においては、データの再生時には、フレーム同期信号（Frame Sync；以下、ＦＳと記す。）により同期をとった後、ＩＤ情報によりセクタ同期をとることによって、１ブロック上のデータの位置が判別できることから、ＩＤ情報は、ディスク状記録媒体上でのデータ方向に配置されている必要がある。また、ＩＤ情報は、各物理セクタ内で同じ位置に配置されている必要がある。そのため、ディスク状記録媒体上に並べられるパリティ以外のデータにおいては、例えばＤＶＤの場合には同図に示すように、ＦＳを記録するためのＦＳ領域が各物理セクタの先頭に位置している。

【０００７】このようなディスク状記録媒体に対するディジタルデータの記録及び／又は再生を行うデータ記録再生装置は、例えば図１８に示すような各部を備える。すなわち、データ記録再生装置１００は、ディスク状記録媒体１５０を回転駆動するスピンドルモータ１０１と、ディスク状記録媒体１５０に対してレーザ光を照射するとともにその戻り光を受光する光学ピックアップ１０２と、この光学ピックアップ１０２におけるレーザダイオードを駆動するレーザドライバ１０３と、光学ピックアップ１０２から出力された信号を電流－電圧変換（ＩＶ変換）して得られたＲＦ（Radio Frequency）信号からデータを検出する信号検出部１０４と、後述するバッファメモリ１０６から読み出したデータを変調するとともに、信号検出部１０４から供給されるデータを復調する変復調部１０５と、データに各種処理を施すためにデータを一時記憶するバッファメモリ１０６と、このバッファメモリ１０６と、変復調部１０５、後述するＥＣＣ部１０８又は後述する入出力部１０９との間で行われるデータの入出力を調停する調停部１０７と、データに対する誤り訂正及び／又は誤り検出を行うＥＣＣ部１０８と、外部とのデータの入出力を行うためのインターフェースである入出力部１０９とを備える。

【０００８】スピンドルモータ１０１は、図示しないサーボ回路の制御の下に、ディスク状記録媒体１５０を所定の回転速度により回転駆動する。

【０００９】光学ピックアップ１０２は、ディスク状記録媒体１５０に対するデータの記録時には、後段のレーザドライバ１０３により駆動された図示しないレーザダイオードからのレーザ光を図示しない対物レンズにより集光してディスク状記録媒体１５０上に照射し、記録すべきデータをピット列としてディスク状記録媒体１５０に記録する。

【００１０】また、光学ピックアップ１０２は、ディスク状記録媒体１５０に記録されているデータの再生時には、図示しないレーザダイオードからのレーザ光を図示しない対物レンズにより集光してディスク状記録媒体１５０上に照射するとともに、ディスク状記録媒体１５０の表面で反射回折された戻り光を図示しないフォトダイオードにより受光して電気信号に変換することによって、ディスク状記録媒体１５０に記録されているデータを読み出す。

【００１１】このような光学ピックアップ１０２は、ディスク状記録媒体１５０に対してデータを記録時及び再生時には、受光した戻り光に基づいて、トラッキング制御やフォーカス制御がされ、ディスク状記録媒体１５０に対してアクセスする。

【００１２】レーザドライバ１０３は、変復調部１０５から供給されるデータに基づいて、光学ピックアップ１０２におけるレーザダイオードを駆動する。

【００１３】信号検出部１０４は、光学ピックアップ１０２から出力された信号を電流－電圧変換して得られたＲＦ信号からクロックを再生し、このクロックを基準としてＲＦ信号を順次処理することによって、データを検出する。信号検出部１０４は、検出したデータを変復調部１０５に供給する。

【００１４】変復調部１０５は、ディスク状記録媒体１５０に対するデータの記録時には、調停部１０７を介してバッファメモリ１０６からＥＣＣブロック単位で記録

すべきデータを読み出し、これらのデータを所定のフォーマットにより変調する。変復調部１０５は、同期信号やその他の情報をデータに付加し、変調して得られたデータをレーザドライバ１０３に供給する。

【００１５】また、変復調部１０５は、ディスク状記録媒体１５０に記録されているデータの再生時には、信号検出部１０４から供給されるデータに対して、ＦＳによるフレーム同期及びブロックアドレスによるブロック同期をとり、これらのフレーム同期及びブロック同期のタイミングを基準にして順次供給されるデータを復調し、調停部１０７を介してバッファメモリ１０６に供給する。

【００１６】バッファメモリ１０６は、ディスク状記録媒体１５０に対するデータの記録時には、入出力部１０９により外部のアプリケーション側から入力されたデータが調停部１０７を介して供給され、このデータを一時記憶する。バッファメモリ１０６により一時記憶されたデータは、調停部１０７を介してＥＣＣ部１０８により読み出される。そして、バッファメモリ１０６は、ＥＣＣ部１０８により誤り訂正符号化されたデータが調停部１０７を介して供給され、このデータを一時記憶する。バッファメモリ１０６により一時記憶されたデータは、調停部１０７を介して変復調部１０５により所定順序で読み出される。

【００１７】また、バッファメモリ１０６は、ディスク状記録媒体１５０に記録されているデータの再生時には、変復調部１０５により復調されたデータが調停部１０７を介して供給され、このデータを一時記憶する。バッファメモリ１０６により一時記憶されたデータは、調停部１０７を介してＥＣＣ部１０８により読み出される。そして、バッファメモリ１０６は、ＥＣＣ部１０８により誤り検出処理されたデータが調停部１０７を介して供給され、このデータを一時記憶する。バッファメモリ１０６により一時記憶されたデータは、調停部１０７を介して入出力部１０９により所定順次で読み出される。

【００１８】調停部１０７は、変復調部１０５、ＥＣＣ部１０８又は入出力部１０９のそれぞれに対してバッファメモリ１０６を使用する占有権を割り当て、バッファメモリ１０６と、変復調部１０５、ＥＣＣ部１０８又は入出力部１０９との間で行われるデータの入出力を調停する。

【００１９】ＥＣＣ部１０８は、ディスク状記録媒体１５０に対するデータの記録時には、入出力部１０９により外部のアプリケーション側から入力されてバッファメモリ１０６により一時記憶されたデータを調停部１０７を介して読み出し、このデータを誤り訂正符号化する。ＥＣＣ部１０８は、誤り訂正符号化したデータを調停部１０７を介してバッファメモリ１０６に供給する。

【００２０】また、ＥＣＣ部１０８は、ディスク状記録媒体１５０に記録されているデータの再生時には、変復調部１０５により復調されバッファメモリ１０６により一時記憶されたデータを調停部１０７を介して読み出し、このデータの誤り検出を行う。ＥＣＣ部１０８は、誤り検出を行ったデータを調停部１０７を介してバッファメモリ１０６に供給する。

【００２１】入出力部１０９は、ディスク状記録媒体１５０に対するデータの記録時には、外部のアプリケーション側から入力されたデータを調停部１０７を介して読み出し、外部のアプリケーション側へ出力する。

【００２２】また、入出力部１０９は、ディスク状記録媒体１５０に記録されているデータの再生時には、ＥＣＣ部１０８により誤り検出が行われてバッファメモリ１０６に一時記憶されているデータを調停部１０７を介して読み出し、外部のアプリケーション側へ出力する。

【００２３】このようなデータ記録再生装置１００は、ディスク状記録媒体１５０に対するデータの記録時には、ディスク状記録媒体１５０に予め形成されているプリピットによる物理アドレスを光学ピックアップ１０２を介して読み出し、変復調部１０５により検出する。データ記録再生装置１００は、この物理アドレスのタイミングを基準にしてディスク状記録媒体１５０に対してＥＣＣブロック単位で順次記録する。

【００２４】また、データ記録再生装置１００は、ディスク状記録媒体１５０に記録されているデータの再生時には、変復調部１０５により物理アドレスを検出し、そのタイミングを基準にしてディスク状記録媒体１５０からＥＣＣブロック単位で順次再生する。

【００２５】【発明が解決しようとする課題】ところで、上述したようなディスク状記録媒体において、当該ディスク状記録媒体に記録されているデータの解読や当該ディスク状記録媒体自体の複製、すなわち、ディスクコピー等に対する措置が考慮されていない方式やフォーマットにより構成されているものは、いかなるデータ記録再生装置であっても記録及び／又は再生され得る。

【００２６】このような現状に鑑みて、近年では、このようなディスク状記録媒体に記録されているデータの解読やディスクコピー等に対する措置が考えられている。

【００２７】例えば、ディスク状記録媒体から正当なデータ記録再生装置のみがデータを再生できるようにするため、上述したＥＣＣ部や変復調部等のデータ処理部と外部のアプリケーション側との間に暗号化部を備えるデータ記録再生装置がある。

【００２８】このデータ記録再生装置は、ディスク状記録媒体の初期化時に、ランダムデータを発生し、このランダムデータをディスク状記録媒体に固有のディスクＩＤとして、ディスク状記録媒体のコントロール領域のデータ中に記録する。そして、このデータ記録再生装置は、ユーザデータの記録時には、ディスクＩＤを用いて

ユーザデータを暗号化してディスク状記録媒体に記録し、ユーザデータの再生時には、再生したデータをディスクＩＤを用いて復号化する。

【００２９】このようにすることによって、暗号化部を備えないデータ記録再生装置は、ディスク状記録媒体から再生したデータを復号化することができない。また、このような方法をとることによって、ディスク状記録媒体のユーザ領域のデータの再生時に復号化せず、又は、暗号化部を通さずに、このデータを、他のディスク状記録媒体に暗号化することなく、又は、暗号化部を通さずに記録した場合でも、ディスクＩＤが異なることから、復号化することができない。

【００３０】しかしながら、このような方法では、初期化したディスク状記録媒体に暗号化したデータを記録し、この暗号化されたデータを復号化せず、又は、暗号化部を通さずに再生するといった手順を繰り返すことによって、不当な第三者は、ディスクＩＤを知ることができる。そのため、不当な第三者は、ディスクＩＤを知ることによって、上述したＥＣＣ部や変復調部等のデータ処理部からの出力に対して復号化できるようになってしまうといった問題があった。

【００３１】また、暗号化部を備えるデータ記録再生装置であっても、ファームウェア等を改変したものでは、再生したデータを復号化できてしまうことが考えられる。ディスクＩＤがわかれば、暗号化部を備えない不当なデータ記録再生装置であっても、そのディスクＩＤを用いて暗号化したデータを生成し、他のディスク状記録媒体に記録することができてしまう。

【００３２】さらに、ディスク状記録媒体のコントロール領域を含む全ての領域のデータを再生する際に、データの復号化を行わず、又は、暗号化部を通さずに、このデータを、他のディスク状記録媒体に暗号化することなく、又は、暗号化部を通さずに記録した場合には、ディスクＩＤも他のディスク状記録媒体にコピーされることとなり、不当なデータ記録再生装置であっても、データを復号化することができてしまう。

【００３３】本発明は、このような実情に鑑みてなされたものであり、ディスク状記録媒体に対する従来の記録及び／又は再生の方式における問題を解決し、ディスク状記録媒体に記録されているデータの解読やディスクコピーを困難とするデータ記録再生方法及びデータ記録再生装置を提供することを目的とするものである。

【００３４】

【課題を解決するための手段】上述した目的を達成する本発明にかかるデータ記録再生方法は、ディスク状記録媒体に対するブロック単位でのデータの記録及び／又は再生を行うデータ記録再生方法であって、ディスク状記録媒体の初期化時に、ディスク状記録媒体に固有の記録媒体識別情報をディスク状記録媒体のコントロール領域における所定領域に記録し、ディスク状記録媒体に対するユーザデータの記録時に、記録媒体識別情報を用いてユーザデータを暗号化することを特徴としている。

【００３５】このような本発明にかかるデータ記録再生方法は、ディスク状記録媒体のコントロール領域における所定領域に記録されているディスク状記録媒体に固有の記録媒体識別情報を用いてユーザデータを暗号化する。

【００３６】また、上述した目的を達成する本発明にかかるデータ記録再生装置は、ディスク状記録媒体に対するブロック単位でのデータの記録及び／又は再生を行うデータ記録再生装置であって、ディスク状記録媒体に対して記録すべきデータを暗号化するとともに、ディスク状記録媒体に記録されている再生すべきデータを復号化する暗号化手段を少なくとも有してデータ処理を行うデータ処理手段を備え、暗号化手段は、ディスク状記録媒体の初期化時に、ディスク状記録媒体に固有の記録媒体識別情報をディスク状記録媒体のコントロール領域における所定領域に記録し、ディスク状記録媒体に対するユーザデータの記録時に、記録媒体識別情報を用いてユーザデータを暗号化することを特徴としている。

【００３７】このような本発明にかかるデータ記録再生装置は、暗号化手段によって、ディスク状記録媒体のコントロール領域における所定領域に記録されているディスク状記録媒体に固有の記録媒体識別情報を用いてユーザデータを暗号化する。

【００３８】

【発明の実施の形態】以下、本発明を適用した具体的な実施の形態について図面を参照しながら詳細に説明する。

【００３９】本発明を適用した実施の形態は、いわゆる光ディスクのようなディスク状記録媒体に対するデータの記録及び／又は再生を行うデータ記録再生装置である。

【００４０】実施の形態として示すデータ記録再生装置に適用されるディスク状記録媒体におけるフォーマットは、図１に示すように、フレーム同期信号（Ｆｒａｍｅ Ｓｙｎｃ；以下、ＦＳと記す。）を記録するためのフレーム同期信号記録領域であるＦＳ領域と、例えばアドレス情報等のデータ以外の付加情報であるＩＤＳを記録するための付加情報記録領域であるＩＤＳ領域と、データであるＵＤＳを記録するためのデータ記録領域であるＵＤＳ領域とにより１ブロックのデータが構成されるものである。ＵＤＳ領域の情報ワードは、データ記録再生装置に対する外部のアプリケーション側との間で入出力される通常のデータ部であり、ＩＤＳ領域の情報ワードは、データ記録再生装置に対する外部のアプリケーション側との間でそのままの形式では入出力されないものである。なお、ディスク状記録媒体においては、このように、ＵＤＳ領域とＩＤＳ領域とに対して、それぞれ、データの入出力等の制御が可能であれば、必ずしも符号ブロック

として区別しなくてもよい。

【００４１】このＩブロックのデータは、同図中斜線部に示すように、例えばＲＳ（Read Solomon Code）により誤り訂正符号化される。例えば、同図に示すように、ＵＤＳは、ＲＳ（２４８，２１６，３３）×３０４符号により構成され、符号の情報ワードは、３０４バイト×２１６バイト＝６５６６４バイト≒約６４Ｋバイトである。また、例えば、同図に示すように、ＩＤＳは、ＲＳ（６２，３０，３３）×２４符号により構成され、符号の情報ワードは、２４バイト×３０バイト＝７２０バイトである。

【００４２】さらに、ディスク状記録媒体には、当該ディスク状記録媒体に固有の記録媒体識別情報であるディスクＩＤ（disk_id）やブロックに固有のブロック識別情報であるブロックＩＤ（blk_id）といったデータを暗号化する際に用いる暗号鍵のＩＤ情報が誤り訂正符号化されて例えばＦＳ領域といった秘匿性のある情報中に記録される。このＩＤ情報は、例えば、ＲＳ（６２，２１６，３３）×１符号により構成され、符号の情報ワードは、１バイト×３０バイト＝３０バイトである。

【００４３】ディスク状記録媒体においては、一般に、ＵＤＳは、数百バイト乃至数十Ｋバイトで構成され、ＩＤＳは、数十バイト乃至数百バイトで構成され、ＩＤ情報は、数十バイトで構成される。

【００４４】このＩブロック分のデータは、４９６フレームから構成され、１フレームは、１５５バイトのデータから構成される。また、各フレームには、ＦＳが付加される。すなわち、ディスク状記録媒体上に並べられるバリティ以外のデータは、図２に示すように、１５５バイト×４９６フレームから構成される。

【００４５】なお、先に図１に示したＵＤＳ及びＩＤＳの情報は、フレーム内のデータであり、ＩＤ情報は、１ビットずつＦＳ領域に記録されるものである。

【００４６】このようなディスク状記録媒体に対するディジタルデータの記録及び／又は再生を行うデータ記録再生装置は、図３に示すような各部を備える。すなわち、データ記録再生装置１０は、ディスク状記録媒体３０を回転駆動するスピンドルモータ１１と、ディスク状記録媒体３０に対してレーザ光を照射するとともにその戻り光を受光する光学ピックアップ手段である光学ピックアップ１２と、この光学ピックアップ１２におけるレーザダイオードを駆動するレーザドライバ１３と、光学ピックアップ１２から出力された信号を電流－電圧変換（ＩＶ変換）して得られたＲＦ（Radio Frequency）信号からデータを検出する信号検出手段である信号検出部１４と、後述するバッファメモリ１６から読み出したデータを変調するとともに、信号検出部１４から供給されるデータを復調する変復調手段である変復調部１５と、データに各種処理を施すためにデータを一時記憶する一時記憶手段であるバッファメモリ１６と、このバッファメモリ１６と、変復調部１５、後述するＥＣＣ部１８、後述する暗号化部１９又は後述する入出力部２０との間で行われるデータの入出力を調停する調停手段である調停部１７と、データに対する誤り訂正及び／又は誤り検出を行う誤り訂正及び／又は誤り検出手段であるＥＣＣ部１８と、バッファメモリ１６から読み出した記録すべきデータを暗号化するとともに、バッファメモリ１６から読み出した再生すべきデータを復号化する暗号化手段である暗号化部１９と、外部とのデータの入出力を行うためのインターフェースとなる入出力手段である入出力部２０と、データに対する暗号化及び復号化に必要となる後述する各種情報を保持する記憶手段であるレジスタ２１、２２とを備える。

【００４７】スピンドルモータ１１は、図示しないサーボ回路の制御の下に、ディスク状記録媒体３０を所定の回転速度により回転駆動する。

【００４８】光学ピックアップ１２は、ディスク状記録媒体３０に対するデータの記録時には、後段のレーザドライバ１３により駆動された図示しないレーザダイオードからのレーザ光を図示しない対物レンズにより集光してディスク状記録媒体３０上に照射し、記録すべきデータをピット列としてディスク状記録媒体３０に記録する。

【００４９】また、光学ピックアップ１２は、ディスク状記録媒体３０に記録されているデータの再生時には、図示しないレーザダイオードからのレーザ光を図示しない対物レンズにより集光してディスク状記録媒体３０上に照射するとともに、ディスク状記録媒体３０の表面で反射回折された戻り光を図示しないフォトダイオードにより受光して電気信号に変換することによって、ディスク状記録媒体３０に記録されているデータを読み出す。

【００５０】このような光学ピックアップ１２は、ディスク状記録媒体３０に対してデータを記録時及び再生時には、受光した戻り光に基づいて、トラッキング制御やフォーカス制御がされ、ディスク状記録媒体３０に対してアクセスする。

【００５１】レーザドライバ１３は、変復調部１５から供給されるデータに基づいて、光学ピックアップ１２におけるレーザダイオードを駆動する。

【００５２】信号検出部１４は、光学ピックアップ１２から出力された信号を電流－電圧変換して得られたＲＦ信号からクロックを再生し、このクロックを基準としてＲＦ信号を順次処理することによって、データを検出する。信号検出部１４は、検出したデータを変復調部１５に供給する。

【００５３】変復調部１５は、ディスク状記録媒体３０に対するデータの記録時には、調停部１７を介してバッファメモリ１６からブロック単位で記録すべきデータを読み出し、これらのデータを所定のフォーマットにより変調する。変復調部１５は、同期信号やバッファメモリ

１６から調停部１７を介して読み出したその他の情報をデータに付加し、変調して得られたデータをレーザドライバ１３に供給する。この際、変復調部１５は、暗号化部１９により生成されてレジスタ２１に保持されている上述したＩＤ情報を読み出す。このＩＤ情報は、レーザドライバ１３に供給するデータに付加される。

【００５４】また、変復調部１５は、ディスク状記録媒体３０に記録されているデータの再生時には、信号検出部１４から供給されるデータに対して、ＦＳによるフレーム同期及びブロックアドレスによるブロック同期をとり、これらのフレーム同期及びブロック同期のタイミングを基準にして順次供給されるデータを復調し、得られたデータやその他の情報を調停部１７を介してバッファメモリ１６に供給する。

【００５５】バッファメモリ１６は、ディスク状記録媒体３０に対するデータの記録時には、入出力部２０により外部のアプリケーション側から入力されたデータが調停部１７を介して供給され、このデータを一時記憶する。バッファメモリ１６により一時記憶されたデータは、調停部１７を介して暗号化部１９により読み出される。そして、バッファメモリ１６は、暗号化部１９により暗号化されたデータが調停部１７を介して供給され、このデータを一時記憶する。バッファメモリ１６により一時記憶されたデータは、調停部１７を介してＥＣＣ部１８により読み出される。そして、バッファメモリ１６は、ＥＣＣ部１８により誤り訂正符号化されたデータが調停部１７を介して供給され、このデータを一時記憶する。バッファメモリ１６により一時記憶されたデータは、調停部１７を介して変復調部１５により所定順序で読み出される。

【００５６】また、バッファメモリ１６は、ディスク状記録媒体３０に記録されているデータの再生時には、変復調部１５により復調されたデータが調停部１７を介して供給され、このデータを一時記憶する。バッファメモリ１６により一時記憶されたデータは、調停部１７を介してＥＣＣ部１８により誤り検出処理されたデータが調停部１７を介して供給され、このデータを一時記憶する。バッファメモリ１６により一時記憶されたデータは、調停部１７を介して暗号化部１９により読み出される。そして、バッファメモリ１６は、暗号化部１９により復号化されたデータが調停部１７を介して供給され、このデータを一時記憶する。バッファメモリ１６により一時記憶されたデータは、調停部１７を介して入出力部２０により所定順次で読み出される。

【００５７】調停部１７は、変復調部１５、ＥＣＣ部１８、暗号化部１９又は入出力部２０のそれぞれに対してバッファメモリ１６を使用する占有権を割り当て、バッファメモリ１６と、変復調部１５、ＥＣＣ部１８、暗号化部１９又は入出力部２０との間で行われるデータの入出力を調停する。

【００５８】ＥＣＣ部１８は、ディスク状記録媒体３０に対するデータの記録時には、暗号化部１９により暗号化されてバッファメモリ１６により一時記憶されたデータを調停部１７を介して読み出し、このデータを誤り訂正符号化する。ＥＣＣ部１８は、誤り訂正符号化したデータを調停部１７を介してバッファメモリ１６に供給する。

【００５９】また、ＥＣＣ部１８は、ディスク状記録媒体３０に記録されているデータの再生時には、変復調部１５により復調されてバッファメモリ１６により一時記憶されたデータを調停部１７を介して読み出し、このデータの誤り検出を行う。ＥＣＣ部１８は、誤り検出を行ったデータを調停部１７を介してバッファメモリ１６に供給する。

【００６０】暗号化部１９は、例えば、上述したディスク状記録媒体３０に固有のディスクＩＤ（disk_id）となるランダムデータの発生、データを暗号化する際に用いる鍵情報の生成・分割、データの暗号化・復号化といった処理に関わる演算を行う。

【００６１】暗号化部１９は、ディスク状記録媒体３０に対するデータの記録時には、入出力部２０により外部のアプリケーション側から入力されてバッファメモリ１６により一時記憶されたデータを調停部１７を介して読み出し、このデータを暗号化する。暗号化部１９は、暗号化したデータを調停部１７を介してバッファメモリ１６に供給する。

【００６２】また、暗号化部１９は、ディスク状記録媒体３０に記録されているデータの再生時には、ＥＣＣ部１８により誤り検出されてバッファメモリ１６により一時記憶されたデータを調停部１７を介して読み出し、このデータを復号化する。暗号化部１９は、復号化したデータを調停部１７を介してバッファメモリ１６に供給する。

【００６３】入出力部２０は、ディスク状記録媒体３０に対するデータの記録時には、外部のアプリケーション側から入力されたデータを調停部１７を介してバッファメモリ１６に供給する。

【００６４】また、入出力部２０は、ディスク状記録媒体３０に記録されているデータの再生時には、暗号化部１９により復号化されてバッファメモリ１６に一時記憶されているデータを調停部１７を介して読み出し、後述するように、暗号化部１９の制御の下に、外部のアプリケーション側へと出力する。

【００６５】レジスタ２１は、暗号化部１９により生成された上述したＩＤ情報を保持する。

【００６６】レジスタ２２は、暗号化部１９により生成された暗号化の際に用いる鍵情報を保持する。

【００６７】このようなデータ記録再生装置１０は、上述したＩＤ情報が外部との間で入出力されることは好ま

しくないことから、これらの各部のうち、少なくとも、変復調部１５、調停部１７、ＥＣＣ部１８、暗号化部１９、入出力部２０及びレジスタ２１，２２がチップ化され、データ処理を行うデータ処理手段であるデータ処理部として構成される。このように暗号化部１９をデータ処理部内に構成することによって、データ記録再生装置１０は、図１及び図２に示したようなフォーマットのディスク状記録媒体３０に対するデータの記録及び／又は再生を行うことができる。なお、同図において、dataは、後述するcont_data,controll_data,user_data,blk_dataのうちのいずれか、すなわち、各種データを総称するものであり、infoは、後述するdisk_info,blk_infoのうちのいずれか、すなわち、各種情報を総称するものであり、idは、後述するdisk_id,blk_idのうちのいずれか、すなわち、ＩＤ情報を総称するものであり、keyは、後述するdisk_key,blk_keyのうちのいずれか、すなわち、鍵情報を総称するものである。

【００６８】以下、データ記録再生装置１０における基本的な動作について説明する。

【００６９】まず、データ記録再生装置１０がディスク状記録媒体３０を初期化する場合について説明する。

【００７０】データ記録再生装置１０は、図４に示すように、ステップＳ１において、暗号化部１９によりランダムデータを発生し、このランダムデータをディスク状記録媒体３０に固有のディスクＩＤ（disk_id）とする。データ記録再生装置１０は、このdisk_idをレジスタ２１に供給して保持させる。

【００７１】続いて、データ記録再生装置１０は、ステップＳ２において、図示しないＣＰＵ（Central Processing Unit）及び図示しないインターフェースにより設定されてバッファメモリ１６に保持されているディスク状記録媒体３０に関する情報（disk_info）を調停部１７を介して暗号化部１９に供給し、暗号化部１９によって、disk_idとdisk_infoとを用いてディスク状記録媒体３０に記録するデータを暗号化するための鍵情報（disk_key）を生成する。データ記録再生装置１０は、このdisk_keyをレジスタ２２に供給して保持させる。

【００７２】続いて、データ記録再生装置１０は、ステップＳ３において、入出力部２０により外部のアプリケーション側から入力されてバッファメモリ１６に保持されている制御データ（controll_data）、すなわち、ディスク状記録媒体３０のコントロール領域に記録すべきデータを調停部１７を介して暗号化部１９に供給し、暗号化部１９によって、controll_dataをdisk_keyを用いて暗号化する。データ記録再生装置１０は、この暗号化して得られた暗号化制御データ（cont_data）を調停部１７を介してバッファメモリ１６に供給して保持させる。なお、コントロール領域は、例えばディスク状記録媒体３０の最内周側及び／又は最外周側に設けられる領域である。

【００７３】続いて、データ記録再生装置１０は、ステップＳ４において、ＥＣＣ部１８によって、レジスタ２１に保持されているdisk_idと、バッファメモリ１６に保持されているdisk_info,cont_dataとを読み出し、これらのdisk_id,disk_info,cont_dataに対して誤り訂正符号化を行う。データ記録再生装置１０は、誤り訂正符号化したdisk_idをレジスタ２１に供給して保持させるとともに、誤り訂正符号化したdisk_info,cont_dataを調停部１７を介してバッファメモリ１６に供給して保持させる。

【００７４】続いて、データ記録再生装置１０は、ステップＳ５において、変復調部１５によって、レジスタ２１に保持されているdisk_idと、バッファメモリ１６に保持されているdisk_info,cont_dataとを読み出し、disk_info,cont_dataを所定のフォーマットにより変調するとともに、disk_idをＦＳ中に挿入する。

【００７５】そして、データ記録再生装置１０は、ステップＳ６において、ディスク状記録媒体３０のフォーマットにしたがうブロック構成となったこれらのdisk_id,disk_info,cont_dataをレーザドライバ１３に供給し、光学ピックアップ１２によりブロック単位でディスク状記録媒体３０のコントロール領域に記録する。なお、infoは、ディスク状記録媒体３０における例えばＩＤSといった通常ユーザがアクセスできないデータ上に記録される。

【００７６】このようにして、データ記録再生装置１０は、ディスク状記録媒体３０を初期化する。

【００７７】つぎに、データ記録再生装置１０がディスク状記録媒体３０に対してユーザデータ（user_data）を記録する場合について説明する。

【００７８】データ記録再生装置１０は、ディスク状記録媒体３０の初期化後に当該ディスク状記録媒体３０を交換していない場合には、レジスタ２２に保持されているdisk_keyを用いて記録すべきデータを暗号化する。

【００７９】一方、データ記録再生装置１０は、ディスク状記録媒体３０の初期化後に当該ディスク状記録媒体３０と異なるディスク状記録媒体に交換した場合には、レジスタ２２に保持されているdisk_keyを用いることはできない。

【００８０】そこでまず、データ記録再生装置１０は、図５に示すように、ステップＳ１１において、交換されて図示しない装着部に装着されたディスク状記録媒体３０のコントロール領域中のブロックを再生する。

【００８１】続いて、データ記録再生装置１０は、ステップＳ１２において、変復調部１５によりディスク状記録媒体３０から読み出したdisk_info,cont_dataを復調し、調停部１７を介してバッファメモリ１６に供給して保持させるとともに、変復調部１５によりＦＳ領域から抽出したdisk_idをレジスタ２１に供給して保持させる。

【００８２】続いて、データ記録再生装置１０は、ステップＳ１３において、ＥＣＣ部１８によって、レジスタ２１からdisk_idを読み出すとともに、バッファメモリ１６から調停部１７を介してdisk_info,cont_dataを読み出し、これらのdisk_id,disk_info,cont_dataの誤り検出を行う。データ記録再生装置１０は、誤り検出したdisk_idをレジスタ２１に供給して保持させるとともに、誤り検出したdisk_info,cont_dataを調停部１７を介してバッファメモリ１６に供給して保持させる。

【００８３】続いて、データ記録再生装置１０は、ステップＳ１４において、暗号化部１９によって、レジスタ２１からdisk_idを読み出すとともに、バッファメモリ１６から調停部１７を介してdisk_infoを読み出し、これらのdisk_idとdisk_infoとを用いてdisk_keyを生成する。データ記録再生装置１０は、生成したdisk_keyをレジスタ２２に供給して保持させる。

【００８４】続いて、データ記録再生装置１０は、ステップＳ１５において、暗号化部１９によりランダムデータを発生し、このランダムデータをディスク状記録媒体３０のブロックに固有のブロックＩＤ（blk_id）とする。データ記録再生装置１０は、このblk_idをレジスタ２１に供給して保持させる。

【００８５】続いて、データ記録再生装置１０は、ステップＳ１６において、図示しないＣＰＵ及び図示しないインターフェースにより設定されてバッファメモリ１６に保持されているディスク状記録媒体３０のブロックに関する情報（blk_info）を調停部１７を介して暗号化部１９に供給するとともに、disk_keyをレジスタ２２から暗号化部１９に供給し、暗号化部１９によって、disk_keyとblk_infoと、さらに必要に応じてblk_idとを用いてディスク状記録媒体３０のブロックに記録するデータを暗号化するための鍵情報（blk_key）を生成する。データ記録再生装置１０は、このblk_keyをレジスタ２２に供給して保持させる。

【００８６】続いて、データ記録再生装置１０は、ステップＳ１７において、暗号化部１９によって、入出力部２０により外部のアプリケーション側から入力されてバッファメモリ１６により一時記憶されたuser_dataを調停部１７を介して読み出し、このuser_dataをblk_keyを用いて暗号化する。データ記録再生装置１０は、この暗号化して得られた暗号化ユーザデータ（blk_data）を調停部１７を介してバッファメモリ１６に供給して保持させる。

【００８７】続いて、データ記録再生装置１０は、ステップＳ１８において、ＥＣＣ部１８によって、バッファメモリ１６に保持されているblk_info,blk_dataと、必要に応じてレジスタ２１に保持されているblk_idとを読み出し、これらのblk_info,blk_data,blk_idに対して誤り訂正符号化を行う。データ記録再生装置１０は、誤り訂正符号化したblk_info,blk_dataを調停部１７を介してバッファメモリ１６に供給して保持させるとともに、誤り訂正符号化したblk_idをレジスタ２１に供給して保持させる。

【００８８】続いて、データ記録再生装置１０は、ステップＳ１９において、変復調部１５によって、バッファメモリ１６に保持されているblk_info,blk_dataと、レジスタ２１に保持されているblk_idとを読み出し、blk_info,blk_dataを所定のフォーマットにより変調するとともに、blk_idをＦＳ中に挿入する。

【００８９】そして、データ記録再生装置１０は、ステップＳ２０において、ディスク状記録媒体３０のフォーマットにしたがうブロック構成となったこれらのblk_info,blk_data,blk_idをレーザドライバ１３に供給し、光学ピックアップ１２によりブロック単位でディスク状記録媒体３０のユーザ領域に記録する。なお、infoは、ディスク状記録媒体３０における例えばＩＤＳといった通常ユーザがアクセスできないデータ上に記録される。

【００９０】このようにして、データ記録再生装置１０は、ディスク状記録媒体３０に対してユーザデータを記録する。

【００９１】つぎに、データ記録再生装置１０がディスク状記録媒体３０に記録されているユーザデータを再生する場合について説明する。

【００９２】データ記録再生装置１０は、ディスク状記録媒体３０に対するユーザデータの記録時と同様に、レジスタ２１にdisk_idを保持しているものとする。

【００９３】そして、データ記録再生装置１０は、図６に示すように、ステップＳ２１において、ディスク状記録媒体３０のユーザ領域の所望のブロックを再生する。

【００９４】続いて、データ記録再生装置１０は、ステップＳ２２において、変復調部１５によりディスク状記録媒体３０から読み出したblk_info,blk_dataを復調し、調停部１７を介してバッファメモリ１６に供給して保持させる。また、データ記録再生装置１０は、必要に応じて、変復調部１５によりblk_idをＦＳ領域から抽出し、抽出したblk_idをレジスタ２１に供給して保持させる。

【００９５】続いて、データ記録再生装置１０は、ステップＳ２３において、ＥＣＣ部１８によって、バッファメモリ１６から調停部１７を介してblk_info,blk_dataを読み出すとともに、必要に応じて、レジスタ２１からblk_idを読み出し、これらのblk_info,blk_data,blk_idの誤り検出を行う。データ記録再生装置１０は、誤り検出したblk_info,blk_dataを調停部１７を介してバッファメモリ１６に供給して保持させるとともに、blk_idをレジスタ２１に供給して保持させる。

【００９６】続いて、データ記録再生装置１０は、ステップＳ２４において、暗号化部１９によって、バッファメモリ１６から調停部１７を介してblk_infoを読み出すとともに、必要に応じて、レジスタ２１からblk_idを読

み出し、さらにレジスタ２２からdisk_keyを読み出し、これらのblk_infoとdisk_keyと、さらに必要に応じてblk_idとを用いてblk_keyを生成する。データ記録再生装置１０は、生成したblk_keyをレジスタ２２に供給して保持させる。

【００９７】続いて、データ記録再生装置１０は、ステップＳ２５において、暗号化部１９によって、バッファメモリ１６により一時記憶されたblk_dataを調停部１７を介して読み出し、このblk_dataをblk_keyを用いて復号化する。データ記録再生装置１０は、この復号化して得られたuser_dataを調停部１７を介してバッファメモリ１６に供給して保持させる。

【００９８】そして、データ記録再生装置１０は、ステップＳ２６において、入出力部２０によって、バッファメモリ１６により一時記憶されたuser_dataを調停部１７を介して読み出し、暗号化部１９の制御の下に、外部のアプリケーション側へと出力する。

【００９９】このようにして、データ記録再生装置１０は、ディスク状記録媒体３０に記録されているユーザデータを再生する。

【０１００】なお、データ記録再生装置１０においては、infoは、入出力部２０を介して入出力を行わず、図示しないＣＰＵにより設定された必要な情報のみが図示しないインターフェースを介して入出力される。

【０１０１】以下、このようなデータ記録再生装置１０における暗号化部１９の具体的な動作について図７乃至図１４を用いて説明する。

【０１０２】まず、データ記録再生装置１０における第１の実施の形態について図７を用いて説明する。この第１の実施の形態は、データ記録再生装置１０は、disk_idを用いてデータを暗号化するものである。同図には、ユーザ領域及びコントロール領域のそれぞれにおける例えば３０バイト程度の任意のバイト数を有するＦＳ、７２０バイトのＩＤＳ及び６４ＫバイトのＵＤＳにより構成される１ブロックのデータを示すとともに、これらのＦＳ領域、ＩＤＳ領域及びＵＤＳ領域に対して暗号化部１９における各部により入出力される各種情報を示している。なお、１ブロックのデータには、バリティは含まれていない。

【０１０３】データ記録再生装置１０において、暗号化部１９は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部ｒ（）と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部ｆ（）及びユーザ領域用鍵情報生成手段である鍵情報生成部ｆ’（）と、暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段である暗号化／復号化部ｅ（）及びユーザ領域用暗号化及び／又は復号化手段である暗号化／復号化部ｅ’（）とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、鍵情報生成部ｆ（），ｆ’（），暗号化／復号化部ｅ（），ｅ’（）は、それぞれ、共通化されてもよい。

【０１０４】このような暗号化部１９は、ディスク状記録媒体３０の初期化時には、ランダムデータ発生部ｒ（）によりランダムデータを発生させ、このランダムデータを、上述したように、ディスク状記録媒体３０に固有のdisk_idとし、コントロール領域のブロック内のデータ部以外のＦＳ領域に記録する。

【０１０５】また、暗号化部１９は、初期化時におけるディスク状記録媒体３０に関する各種情報（初期化時情報）であるinfo_dの全部又は一部の情報（記録媒体情報）を、図示しないＣＰＵによりdisk_infoとして設定され、コントロール領域のブロック内のＩＤＳ領域に記録する。なお、初期化時におけるディスク状記録媒体３０に関する各種情報とは、例えば、ディスク状記録媒体３０の利用者情報やパスワード、ディスク状記録媒体３０の初期化に用いる装置やファームウェアや初期化ツールのバージョン、ディスク状記録媒体３０のブリマスタ情報といったものである。

【０１０６】そして、暗号化部１９は、鍵情報生成部ｆ（）によって、disk_idとdisk_infoとを用いて記録媒体鍵情報であるdisk_keyを生成する。

【０１０７】さらに、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ（）によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のＵＤＳ領域に記録する。

【０１０８】なお、暗号化部１９は、一般に、コントロール領域への各種情報の記録を複数ブロックにわたり行う。ただし、データ記録再生装置１０においては、disk_idがディスク状記録媒体３０に対して１つであるため、暗号化部１９は、ランダムデータをランダムデータ発生部ｒ（）により１回のみ発生する。

【０１０９】暗号化部１９は、ディスク状記録媒体３０の初期化時には、このように動作する。

【０１１０】また、暗号化部１９は、ディスク状記録媒体３０に対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部ｆ（）によりdisk_keyを生成する。

【０１１１】そして、暗号化部１９は、記録時におけるディスク状記録媒体３０に関する各種情報（記録時情報）であるinfo_bの全部又は一部の情報（ブロック情報）を、図示しないＣＰＵによりblk_infoとして設定され、ユーザ領域のブロック内のＩＤＳ領域に記録する。なお、記録時におけるディスク状記録媒体３０に関する各種情報とは、例えば、コンテンツの著作権情報やコピー世代管理情報、ユーザデータの記録時に用いる装置やファームウェアのバージョン、アプリケーション側からの制御情報といったものである。

【００１２】さらに、暗号化部１９は、鍵情報生成部ｆ’（）によって、disk_keyとblk_infoとを用いてブロック鍵情報であるblk_keyを生成する。

【００１３】そして、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ’（）によりblk_keyを用いてuser_dataを暗号化し、blk_dataとしてユーザ領域のブロック内のＵＤＳ領域に記録する。

【００１４】暗号化部１９は、ディスク状記録媒体３０に対するユーザデータの記録時には、このように動作する。

【００１５】さらに、暗号化部１９は、ディスク状記録媒体３０に記録されているユーザデータの再生時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部ｆ（）によりdisk_keyを生成する。

【００１６】そして、暗号化部１９は、ユーザ領域のブロックを再生し、再生されたユーザ領域のブロックからblk_infoを取り出し、disk_keyとblk_infoとを用いて鍵情報生成部ｆ’（）によりblk_keyを生成する。

【００１７】また、暗号化部１９は、再生されたユーザ領域のブロックからのblk_dataを、必要に応じて、暗号化／復号化部ｅ’（）によりblk_keyを用いて復号化し、user_dataとして外部のアプリケーション側へと出力する。

【００１８】なお、ユーザ領域のブロックから取り出されたblk_infoは、アプリケーション側に直接出力されることはない。blk_infoは、必要な場合に、必要な情報のみ、例えば図示しないＣＰＵを介して、或いは、専用の信号線を用いて出力され、例えば暗号化されたコンテンツの復号化のために用いられる。

【００１９】暗号化部１９は、ディスク状記録媒体３０に記録されているユーザデータの再生時には、このように動作する。

【００２０】データ記録再生装置１０は、このように暗号化部１９が動作することによって、disk_idに基づいて生成されたdisk_key,blk_keyを用いてデータを暗号化することができ、データの解読やディスクコピーを困難とすることができる。

【００２１】つぎに、データ記録再生装置１０における第２の実施の形態について図８を用いて説明する。この第２の実施の形態は、データ記録再生装置１０は、disk_idの他にblk_idをも用いてデータを暗号化し、blk_keyを解読されにくいように各ブロック毎に変えられるようにするものである。すなわち、この第２の実施の形態では、第１の実施の形態として示したように、disk_keyのみでデータを暗号化するのではない。同図には、ユーザ領域及びコントロール領域のそれぞれにおけるＦＳ、７２０バイトのＩＤＳ及び８４Ｋバイトの ＵＤＳにより構成される１ブロックのデータを示すとともに、これらのＦＳ領域、ＩＤＳ領域及びＵＤＳ領域に対して暗号化部１９における各部により入出力される各種情報を示している。なお、１ブロックのデータには、パリティは含まれていない。

【００２２】データ記録再生装置１０において、暗号化部１９は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部ｒ（）及びユーザ領域用ランダムデータ発生手段であるランダムデータ発生部ｒ’（）と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部ｆ（）及びユーザ領域用鍵情報生成手段である鍵情報生成部ｆ’（）と、暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段である暗号化／復号化部ｅ（）及びユーザ領域用暗号化及び／又は復号化手段である暗号化／復号化部ｅ’（）とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、ランダムデータ発生部ｒ（），ｒ’（），鍵情報生成部ｆ（），ｆ’（）、暗号化／復号化部ｅ（），ｅ’（）は、それぞれ、共通化されてもよい。

【００２３】このような暗号化部１９は、ディスク状記録媒体３０の初期化時には、上述した第１の実施の形態として説明したものと同様の動作を行う。すなわち、暗号化部１９は、ランダムデータ発生部ｒ（）によりランダムデータを発生させ、このランダムデータを、上述したように、ディスク状記録媒体３０に固有のdisk_idとし、コントロール領域のブロック内のデータ部以外のＦＳ領域に記録する。

【００２４】また、暗号化部１９は、初期化時におけるディスク状記録媒体３０に関する各種情報であるinfo_dの全部又は一部の情報を、図示しないＣＰＵによりdisk_infoとして設定され、コントロール領域のブロック内のＩＤＳ領域に記録する。

【００２５】そして、暗号化部１９は、鍵情報生成部ｆ（）によって、disk_idとdisk_infoとを用いてdisk_keyを生成する。

【００２６】さらに、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ（）によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のＵＤＳ領域に記録する。

【００２７】暗号化部１９は、ディスク状記録媒体３０の初期化時には、このように動作する。

【００２８】また、暗号化部１９は、ディスク状記録媒体３０に対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部ｆ（）によりdisk_keyを生成する。

【００２９】そして、暗号化部１９は、ランダムデータ発生部ｒ’（）によりランダムデータを発生させ、このランダムデータを、ディスク状記録媒体３０のブロックに固有のblk_idとし、ユーザ領域のブロック内のデータ

部以外のＦＳ領域に記録する。

【０１３０】さらに、暗号化部１９は、記録時におけるディスク状記録媒体３０に関する各種情報であるinfo_bの全部又は一部の情報を、図示しないＣＰＵによりblk_infoとして設定され、ユーザ領域のブロック内のＩＤＳ領域に記録する。

【０１３１】また、暗号化部１９は、鍵情報生成部ｆ’（）によって、disk_keyとblk_idとblk_infoとを用いてblk_keyを生成する。

【０１３２】そして、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ’（）によりblk_keyを用いてuser_dataを暗号化し、blk_dataとしてユーザ領域のブロック内のＵＤＳ領域に記録する。

【０１３３】暗号化部１９は、ディスク状記録媒体３０に対するユーザデータの記録時には、このように動作する。

【０１３４】さらに、暗号化部１９は、ディスク状記録媒体３０に記録されているユーザデータの再生時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部ｆ（）によりdisk_keyを生成する。

【０１３５】そして、暗号化部１９は、ユーザ領域のブロックを再生し、再生されたユーザ領域のブロックからblk_idとblk_infoとを取り出し、disk_keyとblk_idとblk_infoとを用いて鍵情報生成部ｆ’（）によりblk_keyを生成する。

【０１３６】また、暗号化部１９は、再生されたユーザ領域のブロックからのblk_dataを、必要に応じて、暗号化／復号化部ｅ’（）によりblk_keyを用いて復号化し、user_dataとして外部のアプリケーション側へと出力する。

【０１３７】暗号化部１９は、ディスク状記録媒体３０に記録されているユーザデータの再生時には、このように動作する。

【０１３８】ディスク状記録媒体３０においては、disk_keyが固定であるとともに、blk_infoも一定となることがある。すなわち、blk_infoのもとhowever info_bは、上述したように、コンテンツの著作権情報やコピー世代管理情報といったコンテンツ単位の情報である場合がある。そのため、例えば動画データ等の多くのブロックに記録されるコンテンツが記録されたブロックに関するinfo_bは、ブロック間で一定となる。データ記録再生装置１０は、このような場合にも効果を奏するものであり、図８に示したように暗号化部１９が動作することによって、blk_keyを解読されにくいように各ブロック毎に変えることができることから、disk_id,blk_idに基づいて生成されたdisk_key,blk_keyを用いてデータを暗号化することができ、データの解読やディスクコピーを困難とすることができる。

【０１３９】つぎに、データ記録再生装置１０における第３の実施の形態について図９を用いて説明する。この第３の実施の形態は、データ記録再生装置１０は、disk_info,blk_infoもそれぞれdisk_id,blk_idを用いて暗号化するものである。すなわち、この第３の実施の形態は、info_d,info_bが不当な第三者に知られることを防止するものである。同図には、ユーザ領域及びコントロール領域のそれぞれにおけるＦＳ、７２０バイトのＩＤＳ及び６４Ｋバイトの ＵＤＳにより構成される１ブロックのデータを示すとともに、これらのＦＳ領域、ＩＤＳ領域及びＵＤＳ領域に対して暗号化部１９における各部により入出力される各種情報を示している。なお、１ブロックのデータには、パリティは含まれていない。

【０１４０】データ記録再生装置１０において、暗号化部１９は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部ｒ（）及びユーザ領域用ランダムデータ発生手段であるランダムデータ発生部ｒ’（）と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部ｆ（）及びユーザ領域用鍵情報生成手段である鍵情報生成部ｆ’（）と、暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段である暗号化／復号化部ｅ（）及びユーザ領域用暗号化及び／又は復号化手段である暗号化／復号化部ｅ’（）とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、ランダムデータ発生部ｒ（）、ｒ’（）、鍵情報生成部ｆ（）、ｆ’（）、暗号化／復号化部ｅ（）、ｅ’（）は、それぞれ、共通化されてもよい。

【０１４１】このような暗号化部１９は、ディスク状記録媒体３０の初期化時には、ランダムデータ発生部ｒ（）によりランダムデータを発生させ、このランダムデータを、上述したように、ディスク状記録媒体３０に固有のdisk_idとし、コントロール領域のブロック内のデータ部以外のＦＳ領域に記録する。

【０１４２】また、暗号化部１９は、必要に応じて鍵情報生成部ｆ（）によって、disk_id、初期化時におけるディスク状記録媒体３０に関する各種情報であるinfo_dの全部又は一部の情報とを用いてdisk_keyを生成する。暗号化部１９は、生成したdisk_keyをdisk_infoとしてコントロール領域のブロック内のＩＤＳ領域に記録する。

【０１４３】そして、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ（）によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のＵＤＳ領域に記録する。

【０１４４】暗号化部１９は、ディスク状記録媒体３０の初期化時には、このように動作する。

【０１４５】また、暗号化部１９は、ディスク状記録媒体３０に対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、鍵情報生成部ｆ（）に

よりdisk_infoを取り出してdisk_keyを生成する。

【０１４６】そして、暗号化部１９は、ランダムデータ発生部ｒ’（）によりランダムデータを発生させ、このランダムデータを、ディスク状記録媒体３０のブロックに固有のblk_idとして、ユーザ領域のブロック内のデータ部以外のＦＳ領域に記録する。

【０１４７】さらに、暗号化部１９は、必要に応じて鍵情報生成部ｆ’（）によって、disk_keyと、blk_idと、記録時におけるディスク状記録媒体３０に関する各種情報であるinfo_bの全部又は一部の情報とを用いてblk_keyを生成する。暗号化部１９は、生成したblk_keyをblk_infoとしてユーザ領域のブロック内のＩＤＳ領域に記録する。

【０１４８】そして、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ’（）によりblk_keyを用いてuser_dataを暗号化し、b1k_dataとしてユーザ領域のブロック内のＵＤＳ領域に記録する。

【０１４９】暗号化部１９は、ディスク状記録媒体３０に対するユーザデータの記録時には、このように動作する。

【０１５０】さらに、暗号化部１９は、ディスク状記録媒体３０に記録されているユーザデータの再生時には、予めコントロール領域のブロックを再生し、鍵情報生成部ｆ（）によりdisk_infoを取り出してdisk_keyを生成する。

【０１５１】そして、暗号化部１９は、ユーザ領域のブロックを再生し、再生されたユーザ領域のブロックからblk_idとblk_infoとを取り出し、disk_keyとblk_idとblk_infoとを用いて鍵情報生成部ｆ’（）によりblk_keyを生成する。

【０１５２】また、暗号化部１９は、再生されたユーザ領域のブロックからのblk_dataを、必要に応じて、暗号化／復号化部ｅ’（）によりblk_keyを用いて復号化し、user_dataとして外部のアプリケーション側へと出力する。

【０１５３】暗号化部１９は、ディスク状記録媒体３０に記録されているユーザデータの再生時には、このように動作する。

【０１５４】データ記録再生装置１０は、このように暗号化部１９が動作することによって、disk_info,b1k_infoもそれぞれdisk_id,b1k_idを用いて暗号化することができる。そのため、データ記録再生装置１０は、上述したデータ処理部とバッファメモリ１６との間の信号をモニタされることによって、disk_info及びb1k_infoがそれぞれ不当な第三者によりコントロール領域及びユーザ領域のブロック内のＩＤＳ領域から取り出され、info_d及びinfo_bが不当な第三者に知られることを防止することができることから、disk_id,b1k_idに基づいて生成されたdisk_key,b1k_keyを用いてデータを暗号化することができ、データの解読やディスクコピーを困難とすることができる。

【０１５５】つぎに、データ記録再生装置１０における第４の実施の形態について図１０を用いて説明する。この第４の実施の形態は、データ記録再生装置１０は、第３の実施の形態と同様に、disk_info,b1k_infoもそれぞれdisk_id,b1k_idを用いて暗号化するものである。同図には、ユーザ領域及びコントロール領域のそれぞれにおけるＦＳ、７２０バイトのＩＤＳ及び６４Ｋバイトの ＵＤＳにより構成される１ブロックのデータを示すとともに、それらのＦＳ領域、ＩＤＳ領域及びＵＤＳ領域に対して暗号化部１９における各部により入出力される各種情報を示している。なお、１ブロックのデータには、パリティは含まれていない。

【０１５６】データ記録再生装置１０において、暗号化部１９は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部ｒ（）及びユーザ領域用ランダムデータ発生手段であるランダムデータ発生部ｒ’（）と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部ｆ（）及びユーザ領域用鍵情報生成手段である鍵情報生成部ｆ’（）と、暗号化及び／又は復号化を行う第１及び第２のコントロール領域用暗号化及び／又は復号化手段である暗号化／復号化部ｇ（），ｅ（）及び第１及び第２のユーザ領域用暗号化及び／又は復号化手段である暗号化／復号化部ｇ’（），ｅ’（）とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、ランダムデータ発生部ｒ（），ｒ’（）、鍵情報生成部ｆ（），ｆ’（）、暗号化／復号化部ｇ（），ｇ’（）、暗号化／復号化部ｅ（），ｅ’（）は、それぞれ、共通化されてもよい。

【０１５７】このような暗号化部１９は、ディスク状記録媒体３０の初期化時には、ランダムデータ発生部ｒ（）によりランダムデータを発生させ、このランダムデータを、上述したように、ディスク状記録媒体３０に固有のdisk_idとし、コントロール領域のブロック内のデータ部以外のＦＳ領域に記録する。

【０１５８】また、暗号化部１９は、必要に応じて暗号化／復号化部ｇ（）によって、disk_idを用いて、初期化時におけるディスク状記録媒体３０に関する各種情報であるinfo_dの全部又は一部の情報を暗号化し、disk_infoを生成する。暗号化部１９は、生成したdisk_infoをコントロール領域のブロック内のＩＤＳ領域に記録する。

【０１５９】さらに、暗号化部１９は、鍵情報生成部ｆ（）によって、disk_infoをdisk_keyとする。

【０１６０】そして、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ（）によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のＵＤＳ領域に記録する。

【００６１】暗号化部１９は、ディスク状記録媒体３０の初期化時には、このように動作する。

【００６２】また、暗号化部１９は、ディスク状記録媒体３０に対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、disk_infoを取り出して鍵情報生成部ｆ（）によりdisk_keyを生成する。

【００６３】そして、暗号化部１９は、ランダムデータ発生部ｒ’（）によりランダムデータを発生させ、このランダムデータを、ディスク状記録媒体３０のブロックに固有のblk_idとし、ユーザ領域のブロック内のデータ部以外のＦＳ領域に記録する。

【００６４】さらに、暗号化部１９は、必要に応じて暗号化／復号化部ｇ’（）によって、disk_keyとblk_idとを用いて、記録時におけるディスク状記録媒体３０に関する各種情報であるinfo_bの全部又は一部の情報を暗号化し、blk_infoを生成する。暗号化部１９は、生成したblk_infoをユーザ領域のブロック内のＩＤＳ領域に記録する。

【００６５】また、暗号化部１９は、鍵情報生成部ｆ’（）によって、blk_infoをblk_keyとする。

【００６６】そして、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ’（）によりblk_keyを用いてuser_dataを暗号化し、blk_dataとしてユーザ領域のブロック内のＵＤＳ領域に記録する。

【００６７】暗号化部１９は、ディスク状記録媒体３０に対するユーザデータの記録時には、このように動作する。

【００６８】さらに、暗号化部１９は、ディスク状記録媒体３０に記録されているユーザデータの再生時には、予めコントロール領域のブロックを再生し、disk_infoを取り出して鍵情報生成部ｆ（）によりdisk_keyを生成する。

【００６９】そして、暗号化部１９は、ユーザ領域のブロックを再生し、再生されたユーザ領域のブロックからblk_infoを取り出し、disk_keyとblk_infoとを用いて鍵情報生成部ｆ’（）によりblk_keyを生成する。

【００７０】また、暗号化部１９は、再生されたユーザ領域のブロックからのblk_dataを、必要に応じて、暗号化／復号化部ｅ’（）によりblk_keyを用いて復号化し、user_dataとして外部のアプリケーション側へと出力する。

【００７１】暗号化部１９は、ディスク状記録媒体３０に記録されているユーザデータの再生時には、このように動作する。

【００７２】データ記録再生装置１０は、このように暗号化部１９が動作することによって、disk_info,blk_infoもそれぞれdisk_id,blk_idを用いて暗号化することができる。そのため、データ記録再生装置１０は、上述したデータ処理部とバッファメモリ１６との間の信号をモニタされることによって、disk_info及びblk_infoがそれぞれ不当な第三者によりコントロール領域及びユーザ領域のブロック内のＩＤＳ領域から取り出され、info_d及びinfo_bが不当な第三者に知られることを防止することができることから、disk_id,blk_idに基づいて生成されたdisk_key,blk_keyを用いてデータを暗号化することができ、データの解読やディスクコピーを困難とすることができる。

【００７３】つぎに、データ記録再生装置１０における第５の実施の形態について図１１を用いて説明する。この第５の実施の形態では、データ記録再生装置１０は、仮にblk_infoが不当な第三者に知られてもuser_dataが知られることがないものである。同図には、ユーザ領域及びコントロール領域のそれぞれにおけるＦＳ、７２０バイトのＩＤＳ及び６４Ｋバイトの ＵＤＳにより構成される１ブロックのデータを示すとともに、これらのＦＳ領域、ＩＤＳ領域及びＵＤＳ領域に対して暗号化部１９における各部により入出力される各種情報を示している。なお、１ブロックのデータには、バリティは含まれていない。

【００７４】データ記録再生装置１０において、暗号化部１９は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部ｒ（）及びユーザ領域用ランダムデータ発生手段であるランダムデータ発生部ｒ’（）と、鍵情報を分割するコントロール領域用鍵情報分割手段である鍵情報分割部ｄ（）及びユーザ領域用鍵情報分割手段である鍵情報分割部ｄ’（）と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部ｆ（）及びユーザ領域用鍵情報生成手段である鍵情報生成部ｆ’（）と、暗号化及び／又は復号化を行う第１及び第２のコントロール領域用暗号化及び／又は復号化手段である暗号化／復号化部ｇ（），ｅ（）及び第１及び第２のユーザ領域用暗号化及び／又は復号化手段である暗号化／復号化部ｇ’（），ｅ’（）とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、ランダムデータ発生部ｒ（），ｒ’（）、鍵情報分割部ｄ（），ｄ’（）、鍵情報生成部ｆ（），ｆ’（）、暗号化／復号化部ｇ（），ｇ’（）、暗号化／復号化部ｅ（），ｅ’（）は、それぞれ、共通化されてもよい。

【００７５】このような暗号化部１９は、ディスク状記録媒体３０の初期化時には、ランダムデータ発生部ｒ（）によりランダムデータを発生させ、このランダムデータを、上述したように、ディスク状記録媒体３０に固有のdisk_idとし、コントロール領域のブロック内のデータ部以外のＦＳ領域に記録する。

【００７６】また、暗号化部１９は、必要に応じて鍵情報分割部ｄ（）によって、ランダムデータ発生部ｒ（）により発生されたランダムデータを分割する。

【００７７】そして、暗号化部１９は、暗号化／復号化

部ｇ（）によって、鍵情報分割部ｄ（）により分割された一方のランダムデータを用いて、初期化時におけるディスク状記録媒体３０に関する各種情報であるinfo_dの全部又は一部の情報を暗号化し、disk_infoを生成する。暗号化部１９は、生成したdisk_infoをコントロール領域のブロック内のＩＤＳ領域に記録する。

【０１７８】さらに、暗号化部１９は、鍵情報生成部ｆ（）によって、鍵情報分割部ｄ（）により分割された他方のランダムデータと、disk_infoとを用いてdisk_keyを生成する。

【０１７９】なお、暗号化部１９においては、必ずしも鍵情報分割部ｄ（）によりランダムデータ発生部ｒ（）により発生されたランダムデータを分割する必要はなく、ランダムデータ発生部ｒ（）によって、互いに異なる２つのランダムデータを発生し、これら２つのランダムデータをdisk_idとし、一方のランダムデータを用いてdisk_infoを生成するとともに、他方のランダムデータを用いてdisk_keyを生成するようにしてもよい。

【０１８０】そして、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ（）によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のＵＤＳ領域に記録する。

【０１８１】暗号化部１９は、ディスク状記録媒体３０の初期化時には、このように動作する。

【０１８２】また、暗号化部１９は、ディスク状記録媒体３０に対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部ｆ（）によりdisk_keyを生成する。

【０１８３】そして、暗号化部１９は、ランダムデータ発生部ｒ’（）によりランダムデータを発生させ、このランダムデータを、ディスク状記録媒体３０のブロックに固有のblk_idとし、ユーザ領域のブロック内のデータ部以外のＦＳ領域に記録する。

【０１８４】また、暗号化部１９は、必要に応じて鍵情報分割部ｄ’（）によって、ランダムデータ発生部ｒ’（）により発生されたランダムデータを分割する。

【０１８５】さらに、暗号化部１９は、暗号化／復号化部ｇ’（）によって、鍵情報分割部ｄ’（）により分割された一方のランダムデータを用いて、記録時におけるディスク状記録媒体３０に関する各種情報であるinfo_bの全部又は一部の情報を暗号化し、blk_infoを生成する。暗号化部１９は、生成したblk_infoをユーザ領域のブロック内のＩＤＳ領域に記録する。

【０１８６】さらに、暗号化部１９は、鍵情報生成部ｆ’（）によって、鍵情報分割部ｄ’（）により分割された他方のランダムデータと、blk_infoと、disk_keyとを用いてblk_keyを生成する。

【０１８７】なお、暗号化部１９においては、必ずしも鍵情報分割部ｄ’（）によりランダムデータ発生部ｒ’（）により発生されたランダムデータを分割する必要はなく、ランダムデータ発生部ｒ’（）によって、互いに異なる２つのランダムデータを発生し、これら２つのランダムデータをblk_idとし、一方のランダムデータを用いてblk_infoを生成するとともに、他方のランダムデータを用いてblk_keyを生成するようにしてもよい。

【０１８８】そして、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ’（）によりblk_keyを用いてuser_dataを暗号化し、blk_dataとしてユーザ領域のブロック内のＵＤＳ領域に記録する。

【０１８９】暗号化部１９は、ディスク状記録媒体３０に対するユーザデータの記録時には、このように動作する。

【０１９０】さらに、暗号化部１９は、ディスク状記録媒体３０に記録されているユーザデータの再生時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部ｆ’（）によりdisk_keyを生成する。

【０１９１】そして、暗号化部１９は、ユーザ領域のブロックを再生し、再生されたユーザ領域のブロックからblk_idとblk_infoとを取り出し、blk_idとblk_infoとdisk_keyとを用いて鍵情報生成部ｆ’（）によりblk_keyを生成する。

【０１９２】また、暗号化部１９は、再生されたユーザ領域のブロックからのblk_dataを、必要に応じて、暗号化／復号化部ｅ’（）によりblk_keyを用いて復号化し、user_dataとして外部のアプリケーション側へと出力する。

【０１９３】暗号化部１９は、ディスク状記録媒体３０に記録されているユーザデータの再生時には、このように動作する。

【０１９４】データ記録再生装置１０は、このように暗号化部１９が動作することによって、仮にblk_infoが不当な第三者に知られてもuser_dataが知られることがない。そのため、データ記録再生装置１０は、上述したデータ処理部とバッファメモリ１６との間の信号をモニタされることによって、disk_info及びblk_infoがそれぞれ不当な第三者によりコントロール領域及びユーザ領域のブロック内のＩＤＳ領域から取り出されてdisk_key及びblk_keyが不当な第三者に知られた場合にも効果を奏するものであり、disk_key,blk_keyを用いてデータを暗号化することができ、データの解読やディスクコピーを困難とすることができる。

【０１９５】つぎに、データ記録再生装置１０における第６の実施の形態について図１２を用いて説明する。この第６の実施の形態では、データ記録再生装置１０は、コントロール領域内の各ブロックにおいて互いに異なるdisk_idを用いるものである。同図には、ユーザ領域及びコントロール領域のそれぞれにおけるＦＳ、７２０バイトのＩＤＳ及び６４ＫバイトのUDSにより構成され

る１ブロックのデータを示すとともに、これらのＦＳ領域、ＩＤＳ領域及びＵＤＳ領域に対して暗号化部１９における各部により入出力される各種情報を示している。なお、１ブロックのデータには、パリティは含まれていない。

【０１９６】データ記録再生装置１０において、暗号化部１９は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部ｒ（）及びユーザ領域用ランダムデータ発生手段であるランダムデータ発生部ｒ’（）と、鍵情報を分割するコントロール領域用鍵情報分割手段である鍵情報分割部ｄ（）及びユーザ領域用鍵情報分割手段である鍵情報分割部ｄ’（）と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部ｆ（）及びユーザ領域用鍵情報生成手段である鍵情報生成部ｆ’（）と、暗号化及び／又は復号化を行う第１、第２及び第３のコントロール領域用暗号化及び／又は復号化手段である暗号化／復号化部ｂ（），ｇ（），ｅ（）及び第１、第２及び第３のユーザ領域用暗号化及び／又は復号化手段である暗号化／復号化部ｂ’（），ｇ’（），ｅ’（）とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、ランダムデータ発生部ｒ（），ｒ’（）、鍵情報分割部ｄ（），ｄ’（）、鍵情報生成部ｆ（），ｆ’（）、暗号化／復号化部ｂ（），ｂ’（）、暗号化／復号化部ｇ（），ｇ’（）、暗号化／復号化部ｅ（），ｅ’（）は、それぞれ、共通化されてもよい。

【０１９７】このような暗号化部１９は、ディスク状記録媒体３０の初期化時には、ランダムデータ発生部ｒ（）によりランダムデータを発生させ、このランダムデータを、図示しないＣＰＵによって設定された物理ブロック番号（ｂｌｋ_ｎｏ）を用いて、暗号化／復号化部ｂ（）により暗号化し、各ブロック毎に固有のｄｉｓｋ_ｉｄを生成する。暗号化部１９は、生成したｄｉｓｋ_ｉｄをコントロール領域のブロック内のデータ部以外のＦＳ領域に記録する。

【０１９８】また、暗号化部１９は、必要に応じて鍵情報分割部ｄ（）によって、ランダムデータ発生部ｒ（）により発生されたランダムデータを分割する。

【０１９９】そして、暗号化部１９は、暗号化／復号化部ｇ（）によって、鍵情報分割部ｄ（）により分割された一方のランダムデータを用いて、初期化時におけるディスク状記録媒体３０に関する各種情報であるｉｎｆｏ_ｄの全部又は一部の情報を暗号化し、ｄｉｓｋ_ｉｎｆｏを生成する。暗号化部１９は、生成したｄｉｓｋ_ｉｎｆｏをコントロール領域のブロック内のＩＤＳ領域に記録する。

【０２００】さらに、暗号化部１９は、鍵情報生成部ｆ（）によって、鍵情報分割部ｄ（）により分割された他方のランダムデータと、ｄｉｓｋ_ｉｎｆｏとを用いてｄｉｓｋ_ｋｅｙを生成する。

【０２０１】なお、暗号化部１９においては、必ずしも鍵情報分割部ｄ（）によりランダムデータ発生部ｒ（）により発生されたランダムデータを分割する必要はなく、ランダムデータ発生部ｒ（）によって、互いに異なる２つのランダムデータを発生し、これら２つのランダムデータをｄｉｓｋ_ｉｄとし、一方のランダムデータを用いてｄｉｓｋ_ｉｎｆｏを生成するとともに、他方のランダムデータを用いてｄｉｓｋ_ｋｅｙを生成するようにしてもよい。

【０２０２】そして、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ（）によりｄｉｓｋ_ｋｅｙを用いてｃｏｎｔｒｏｌ_ｄａｔａを暗号化し、ｃｏｎｔ_ｄａｔａとしてコントロール領域のブロック内のＵＤＳ領域に記録する。

【０２０３】なお、暗号化部１９は、ｉｎｆｏ_ｄにｂｌｋ_ｎｏが含まれていない場合には、ｄｉｓｋ_ｉｎｆｏやｃｏｎｔ_ｄａｔａをｂｌｋ_ｉｄを用いて暗号化するようにしてもよい。

【０２０４】暗号化部１９は、ディスク状記録媒体３０の初期化時には、このように動作する。

【０２０５】また、暗号化部１９は、ディスク状記録媒体３０に対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、ｄｉｓｋ_ｉｄとｄｉｓｋ_ｉｎｆｏとを取り出して鍵情報生成部ｆ（）によりｄｉｓｋ_ｋｅｙを生成する。

【０２０６】そして、暗号化部１９は、ランダムデータ発生部ｒ’（）によりランダムデータを発生させ、このランダムデータを、図示しないＣＰＵにより設定されたｂｌｋ_ｎｏを用いて、暗号化／復号化部ｂ’（）により暗号化し、各ブロック毎に固有のｂｌｋ_ｉｄを生成する。暗号化部１９は、生成したｂｌｋ_ｉｄをユーザ領域のブロック内のデータ部以外のＦＳ領域に記録する。

【０２０７】また、暗号化部１９は、必要に応じて鍵情報分割部ｄ’（）によって、ランダムデータ発生部ｒ’（）により発生されたランダムデータを分割する。

【０２０８】さらに、暗号化部１９は、暗号化／復号化部ｇ’（）によって、鍵情報分割部ｄ’（）により分割された一方のランダムデータを用いて、記録時におけるディスク状記録媒体３０に関する各種情報であるｉｎｆｏ_ｂの全部又は一部の情報を暗号化し、ｂｌｋ_ｉｎｆｏを生成する。暗号化部１９は、生成したｂｌｋ_ｉｎｆｏをユーザ領域のブロック内のＩＤＳ領域に記録する。

【０２０９】さらに、暗号化部１９は、鍵情報生成部ｆ’（）によって、鍵情報分割部ｄ’（）により分割された他方のランダムデータと、ｂｌｋ_ｉｎｆｏと、ｄｉｓｋ_ｋｅｙとを用いてｂｌｋ_ｋｅｙを生成する。

【０２１０】なお、暗号化部１９においては、必ずしも鍵情報分割部ｄ’（）によりランダムデータ発生部ｒ’（）により発生されたランダムデータを分割する必要はなく、ランダムデータ発生部ｒ’（）によって、互いに異なる２つのランダムデータを発生し、これら２つのランダムデータをｂｌｋ_ｉｄとし、一方のランダムデータを用

いてblk_infoを生成するとともに、他方のランダムデータを用いてblk_keyを生成するようにしてもよい。

【０２１１】そして、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ’（）によりblk_keyを用いてuser_dataを暗号化し、blk_dataとしてユーザ領域のブロック内のＵＤＳ領域に記録する。

【０２１２】なお、暗号化部１９は、各部の共通化を図り、blk_id,blk_info,blk_dataをblk_noを用いて暗号化するようにしてもよい。

【０２１３】暗号化部１９は、ディスク状記録媒体３０に対するユーザデータの記録時には、このように動作する。

【０２１４】さらに、暗号化部１９は、ディスク状記録媒体３０に記録されているユーザデータの再生時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部ｆ（）によりdisk_keyを生成する。

【０２１５】そして、暗号化部１９は、ユーザ領域のブロックを再生し、再生されたユーザ領域のブロックからblk_idとblk_infoとを取り出し、blk_idとblk_infoとdisk_keyとを用いて鍵情報生成部ｆ’（）によりblk_keyを生成する。

【０２１６】また、暗号化部１９は、再生されたユーザ領域のブロックからのblk_dataを、必要に応じて、暗号化／復号化部ｅ’（）によりblk_keyを用いて復号化し、user_dataとして外部のアプリケーション側へと出力する。

【０２１７】暗号化部１９は、ディスク状記録媒体３０に記録されているユーザデータの再生時には、このように動作する。

【０２１８】ディスク状記録媒体３０におけるコントロール領域には、一般に、制御情報が複数ブロックにわたって記録されるが、disk_keyは同一である必要がある。そのため、blk_idやblk_infoが全てのブロック間で同一となり、disk_keyが解読されやすいおそれがある。データ記録再生装置１０は、このような場合にも効果を奏するものであり、図１２に示したように暗号化部１９が動作することによって、コントロール領域内の各ブロックにおいて互いに異なるdisk_idを用いることから、データの解読やディスクコピーを困難とすることができる。

【０２１９】ところで、多数のブロックに記録されるべき暗号化される前のuser_dataと多数のブロックに記録されている暗号化された後のblk_dataとが不当な第三者に知られると、blk_keyが知られるおそれがある。blk_keyが第三者に知られると、user_dataの解読やディスクコピーが可能となる。

【０２２０】そこで、以上のようなデータ記録再生装置１０は、暗号化されたデータを復号化しないで外部のアプリケーション側又は図示しないＣＰＵに出力することを禁止することもできる。この場合、データ記録再生装置１０は、ファームウェアで対処することもできるが、改変される危険性を考慮して、ハードウェアでデータの出力を禁止する。データ記録再生装置１０は、暗号化部１９によって、再生されたdataやinfoが暗号化されているか否かを判別し、入出力制御部２０への出力を制御する。

【０２２１】具体的には、データ記録再生装置１０は、暗号化部１９による判別の結果、controll_data又はuser_dataの再生時に、再生されたブロックからのdisk_id若しくはblk_id又はcont_data若しくはblk_data又はdisk_info若しくはblk_infoが暗号化されていることを示していた場合には、暗号化部１９によって、復号化して出力すべき旨の正しいコマンドを受けた場合にのみ、cont_data若しくはblk_dataを復号化して出力し、復号化しないでそのまま出力すべき旨のコマンドを受けた場合には、cont_data若しくはblk_dataを復号化して出力しない。

【０２２２】一方、データ記録再生装置１０は、暗号化部１９による判別の結果、再生されたブロックからのdisk_id若しくはblk_id又はcont_data若しくはblk_data又はdisk_info若しくはblk_infoが暗号化されていないことを示していた場合には、暗号化部１９によって、復号化して出力すべき旨のコマンドを受けた場合には、cont_data若しくはblk_dataを復号化して出力し、復号化しないでそのまま出力すべき旨のコマンドを受けた場合には、cont_data若しくはblk_dataを復号化して出力する。

【０２２３】さらに、データ記録再生装置１０は、図示しないインターフェースを介してバッファメモリ１６に保持されている各種情報が図示しないＣＰＵに出力されるとともに、図示しないインターフェースを介して図示しないＣＰＵからの各種情報がバッファメモリ１６に供給される。そのため、データ記録再生装置１０は、バッファメモリ１６に保持されているdisk_infoやblk_infoを図示しないＣＰＵに出力することが可能であるが、cont_data若しくはblk_dataと同様に、暗号化部１９による判別に応じて、disk_infoやblk_infoの出力を制御する。

【０２２４】このようにすることによって、データ記録再生装置１０は、user_dataの解読やディスクコピーに対するセキュリティを向上させることができる。

【０２２５】さらに、データ記録再生装置１０においては、上述したように、暗号化部１９をデータ処理部内に構成することによって、先に図１及び図２に示したフォーマットのディスク状記録媒体３０を適用することができ、上述した第１乃至第６の実施の形態として示した方法を用いることができる。これらの場合において、データ処理部とバッファメモリ１６との間の信号をモニタされる危険性があることを述べたが、この危険性に対処するために、データ記録再生装置１０は、バッファメモリ１６をデータ処理部内にチップ化して構成することもで

きる。

【０２２６】このようにすることによって、データ記録再生装置１０は、データ処理部とバッファメモリ１６との間の信号をモニタされる危険性がなくなり、安全性を大幅に向上させることができる。

【０２２７】さらに、データ記録再生装置１０は、必要に応じて、信号検出器１４もデータ処理部内にチップ化して構成することによって、変調前のデータを不当な第三者に知られることがなくなり、より安全なシステムを構築することができる。

【０２２８】なお、バッファメモリ１６をデータ処理部内にチップ化して構成する場合、データ記録再生装置１０においては、レジスタ２１を調停部１７を通してバッファメモリ１６と共通化してもよい。

【０２２９】このように、バッファメモリ１６をデータ処理部内にチップ化して構成することによって、ディスク状記録媒体３０におけるブロック内のデータが外部に漏洩する危険性が小さい場合には、データ記録再生装置１０は、disk_idやblk_idをコントロール領域又はユーザ領域のブロック内のデータ部以外のＦＳ領域に記録する必要はなく、コントロール領域又はユーザ領域のブロック内のＩＤＳ領域に記録するようにしてもよい。この場合、データ記録再生装置１０における暗号化部１９の具体的な動作は、図１３又は図１４に示すようになる。

【０２３０】まず、第７の実施の形態として図１３に示すデータ記録再生装置１０について説明する。同図には、ユーザ領域及びコントロール領域のそれぞれにおけるＦＳ、７２０バイトのＩＤＳ及び６４Ｋバイトのユーザ領域のＵＤＳにより構成される１ブロックのデータを示すとともに、これらのＦＳ領域、ＩＤＳ領域及びＵＤＳ領域に対して暗号化部１９における各部により入出力される各種情報を示している。なお、１ブロックのデータには、パリティは含まれていない。

【０２３１】データ記録再生装置１０において、暗号化部１９は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部ｒ（）と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部ｆ（）及びユーザ領域用鍵情報生成手段である鍵情報生成部ｆ’（）と、暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段である暗号化／復号化部ｅ（）及びユーザ領域用暗号化及び／又は復号化手段である暗号化／復号化部ｅ’（）とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、鍵情報生成部ｆ（），ｆ’（），暗号化／復号化部ｅ（），ｅ’（）は、それぞれ、共通化されてもよい。

【０２３２】このような暗号化部１９は、ディスク状記録媒体３０の初期化時には、ランダムデータ発生部ｒ（）によりランダムデータを発生させ、このランダムデータを、ディスク状記録媒体３０に固有のdisk_idとするとともに、初期化時におけるディスク状記録媒体３０に関する各種情報であるinfo_dの全部又は一部の情報を、図示しないＣＰＵによりdisk_infoとして設定され、これらのdisk_id及びdisk_infoをコントロール領域のブロック内のＩＤＳ領域に記録する。

【０２３３】また、暗号化部１９は、鍵情報生成部ｆ（）によって、disk_idとdisk_infoとを用いてdisk_keyを生成する。

【０２３４】さらに、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ（）によりdisk_keyを用いてcontroll_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のＵＤＳ領域に記録する。

【０２３５】暗号化部１９は、ディスク状記録媒体３０の初期化時には、このように動作する。なお、暗号化部１９は、disk_id及びdisk_infoをコントロール領域のブロック内のＩＤＳ領域に記録するのではなく、cont_dataとともにコントロール領域のブロック内のＵＤＳ領域に記録するようにしてもよい。

【０２３６】また、暗号化部１９は、ディスク状記録媒体３０に対するユーザデータの記録時及びディスク状記録媒体３０に記録されているユーザデータの再生時には、上述した第１の実施の形態と同様に動作する。

【０２３７】さらに、第８の実施の形態として図１４に示すデータ記録再生装置１０について説明する。同図には、ユーザ領域及びコントロール領域のそれぞれにおけるＦＳ、７２０バイトのＩＤＳ及び６４Ｋバイトのユーザ領域のＵＤＳにより構成される１ブロックのデータを示すとともに、これらのＦＳ領域、ＩＤＳ領域及びＵＤＳ領域に対して暗号化部１９における各部により入出力される各種情報を示している。なお、１ブロックのデータには、パリティは含まれていない。

【０２３８】データ記録再生装置１０において、暗号化部１９は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部ｒ（）及びユーザ領域用ランダムデータ発生手段であるランダムデータ発生部ｒ’（）と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部ｆ（）及びユーザ領域用鍵情報生成手段である鍵情報生成部ｆ’（）と、暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段である暗号化／復号化部ｅ（）及びユーザ領域用暗号化及び／又は復号化手段である暗号化／復号化部ｅ’（）とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、ランダムデータ発生部ｒ（），ｒ’（），鍵情報生成部ｆ（），ｆ’（），暗号化／復号化部ｅ（），ｅ’（）は、それぞれ、共通化されてもよい。

【０２３９】このような暗号化部１９は、ディスク状記録媒体３０の初期化時には、ランダムデータ発生部

ｒ（）によりランダムデータを発生させ、このランダムデータを、ディスク状記録媒体３０ｃ固有のdisk_idとするとともに、初期化時におけるディスク状記録媒体３０ｃに関する各種情報であるinfo_dの全部又は一部の情報を、図示しないＣＰＵによりdisk_infoとして設定され、これらのdisk_id及びdisk_infoをコントロール領域のブロック内のＩＤＳ領域に記録する。

【０２４０】また、暗号化部１９は、鍵情報生成部ｆ（）によって、disk_idとdisk_infoとを用いてdisk_keyを生成する。

【０２４１】さらに、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ（）によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のＵＤＳ領域に記録する。

【０２４２】暗号化部１９は、ディスク状記録媒体３０の初期化時には、このように動作する。

【０２４３】また、暗号化部１９は、ディスク状記録媒体３０ｃに対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部ｆ（）によりdisk_keyを生成する。

【０２４４】そして、暗号化部１９は、ランダムデータ発生部ｒ’（）によりランダムデータを発生させ、このランダムデータを、ディスク状記録媒体３０ｃのブロックに固有のblk_idとするとともに、記録時におけるディスク状記録媒体３０ｃに関する各種情報であるinfo_bの全部又は一部の情報を、図示しないＣＰＵによりblk_infoとして設定され、これらのblk_id及びblk_infoをユーザ領域のブロック内のＩＤＳ領域に記録する。

【０２４５】また、暗号化部１９は、鍵情報生成部ｆ’（）によって、disk_keyとblk_idとblk_infoとを用いてblk_keyを生成する。

【０２４６】そして、暗号化部１９は、必要に応じて、暗号化／復号化部ｅ’（）によりblk_keyを用いてuser_dataを暗号化し、blk_dataとしてユーザ領域のブロック内のＵＤＳ領域に記録する。

【０２４７】暗号化部１９は、ディスク状記録媒体３０ｃに対するユーザデータの記録時には、このように動作する。なお、暗号化部１９は、blk_id及びblk_infoをユーザ領域のブロック内のＩＤＳ領域に記録するのではなく、blk_dataとともにユーザ領域のブロック内のＵＤＳ領域に記録するようにしてもよい。

【０２４８】さらに、暗号化部１９は、ディスク状記録媒体３０ｃに記録されているユーザデータの再生時には、上述した第２の実施の形態と同様に動作する。

【０２４９】このように、データ記録再生装置１０は、バッファメモリ１６をデータ処理部内にチップ化して構成することによって、disk_idやblk_idをコントロール領域又はユーザ領域のブロック内のＩＤＳ領域に記録することができ、図１３又は図１４に示したように暗号化部１９が動作することによって、disk_key,blk_keyを用いてデータを暗号化することができ、データの解読やディスクコピーを困難とすることができる。

【０２５０】なお、ここでは、第７及び第８の実施の形態として、バッファメモリ１６をデータ処理部内にチップ化して構成することにより上述した第１及び第２の実施の形態を変化させたデータ記録再生装置１０について説明したが、上述した第３乃至第６の実施の形態についても同様に適用できることはいうまでもない。

【０２５１】また、データ記録再生装置１０において は、定められた暗号フォーマットに対して、一意に構成が定まるのは勿論である。例えば、第８の実施の形態として示した方法を用いる場合には、データ記録再生装置１０は、バッファメモリ１６と暗号化部１９とがデータ処理部内に構成されている必要がある。

【０２５２】さらに、データ記録再生装置１０は、暗号化部１９の内部に図示しないメモリを設け、又は、データ処理部内にバッファメモリ１６を構成し、例えば、disk_infoやblk_infoとして、当該データ記録再生装置１０を製造するメーカの情報（maker_info）や当該データ記録再生装置１０を示す情報（device_info）をディスク状記録媒体３０ｃに記録すべく、各メーカ毎、データ処理部を構成する各ＩＣ（Integrated Circuit）の種類又は世代毎に固有の情報を予めメモリ又はバッファメモリ１６に保持させておくこともできる。これらのmaker_infoやdevice_info等の情報は、例えば、商品化されるデータ記録再生装置におけるデータ処理部によっては出力されないようにしたり、ライセンスを管理するベンダが有するデータ記録再生装置におけるデータ処理部によってのみ出力可能とされる。

【０２５３】このようにすることによって、不当な第三者により違法なデータの解読やディスクコピーがされた場合にも、ディスク状記録媒体３０ｃの初期化やデータの記録がどのような装置や環境により行われたかを示す情報等を得ることができる。

【０２５４】以上説明してきたように、本発明の実施の形態として示すデータ記録再生装置１０は、暗号化された後のデータやデータを暗号化するための各種情報を第三者に知られることを防止することができ、データや鍵情報の解読を困難とすることができる。

【０２５５】また、データ記録再生装置１０は、暗号化及び復号化の方法が公になった場合又は仮にディスク状記録媒体３０ｃに固有の鍵情報が第三者に知られた場合でも、ブロックに固有の鍵情報を用いてデータをブロック毎に暗号化することによって、データの解読を困難とすることができる。

【０２５６】データ記録再生装置１０は、データや鍵情報の解読を困難とすることによって、データの違法なコピーやディスクコピーを防止することができる。さらに、仮に不当な第三者によりデータの違法なコピーやデ

ィスクコピーがされた場合であっても、どのような装置や環境によりディスク状記録媒体３０の初期化やデータの記録が行われたかを示す情報を得ることができ、データの違法なコピーやディスクコピーの防止の一助となる。

【０２５７】なお、本発明は、上述した実施の形態に限定されるものではなく、例えば、いわゆる光ディスクのようなディスク状記録媒体に対するデータの記録及び／又は再生を行うものとして説明したが、データをストレージする記録媒体であれば光ディスク以外の記録媒体にも応用できるものである。

【０２５８】また、上述した実施の形態では、図３に示したデータ記録再生装置１０について説明したが、上述したように、「アプリケーション側との入出力方向」と「暗号化方向」と「ＥＣＣ方向」とが同一であれば、図１５に示すデータ記録再生装置４０であってもよい。

【０２５９】このデータ記録再生装置４０は、上述したスピンドルモータ１１、光学ピックアップ１２、レーザドライバ１３、信号検出部１４、変復調部１５及びバッファメモリ１６の他に、バッファメモリ１６と、変復調部１５、後述するＥＣＣ部４８との間で行われるデータの入出力を調停する調停部４７と、データに対する誤り訂正及び／又は誤り検出を行うＥＣＣ部４８と、後述する入出力部５０から供給される記録すべきデータを暗号化するとともに、ＥＣＣ部４８から供給される再生すべきデータを復号化する暗号化部４９と、外部とのデータの入出力を行うためのインターフェースである入出力部５０と、データに対する暗号化及び復号化に必要となる各種情報を保持するレジスタ５１，５２とを備える。

【０２６０】すなわち、データ記録再生装置４０は、データ記録再生装置１０と比較して、調停部４７によりデータの入出力を調停する必要がある各部が少ない。そのため、データ記録再生装置４０は、調停部４７によるデータの入出力の調停を容易に行うことができる。なお、データ記録再生装置４０によるディスク状記録媒体３０の初期化、ディスク状記録媒体３０に対するユーザデータの記録及びディスク状記録媒体３０に記録されているデータの再生動作は、上述したデータ記録再生装置１０における第１乃至第８の実施の形態と同様であるため、ここでは説明を省略する。

【０２６１】このように、本発明は、その趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。

【０２６２】

【発明の効果】以上詳細に説明したように、本発明にかかるデータ記録再生方法は、ディスク状記録媒体に対するブロック単位でのデータの記録及び／又は再生を行うデータ記録再生方法であって、ディスク状記録媒体の初期化時に、ディスク状記録媒体に固有の記録媒体識別情報をディスク状記録媒体のコントロール領域における所定領域に記録し、ディスク状記録媒体に対するユーザデータの記録時に、記録媒体識別情報を用いてユーザデータを暗号化する。

【０２６３】したがって、本発明にかかるデータ記録再生方法は、ディスク状記録媒体のコントロール領域における所定領域に記録されているディスク状記録媒体に固有の記録媒体識別情報を用いてユーザデータを暗号化することによって、ディスク状記録媒体に記録されているデータの解読やディスクコピーを困難とすることができる。

【０２６４】また、本発明にかかるデータ記録再生装置は、ディスク状記録媒体に対するブロック単位でのデータの記録及び／又は再生を行うデータ記録再生装置であって、ディスク状記録媒体に対して記録すべきデータを暗号化するとともに、ディスク状記録媒体に記録されている再生すべきデータを復号化する暗号化手段を少なくとも有してデータ処理を行うデータ処理手段を備え、暗号化手段は、ディスク状記録媒体の初期化時に、ディスク状記録媒体に固有の記録媒体識別情報をディスク状記録媒体のコントロール領域における所定領域に記録し、ディスク状記録媒体に対するユーザデータの記録時に、記録媒体識別情報を用いてユーザデータを暗号化する。

【０２６５】したがって、本発明にかかるデータ記録再生装置は、暗号化手段によって、ディスク状記録媒体のコントロール領域における所定領域に記録されているディスク状記録媒体に固有の記録媒体識別情報を用いてユーザデータを暗号化することによって、ディスク状記録媒体に記録されているデータの解読やディスクコピーを困難とすることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態として示すデータ記録再生装置に適用されるディスク状記録媒体におけるフォーマットを説明する図であって、１ブロック分を示す図である。

【図２】ディスク状記録媒体におけるフォーマットを説明する図であって、ディスク状記録媒体上に並べられるバリティ以外のデータを示す図である。

【図３】同データ記録再生装置の構成を説明するブロック図である。

【図４】同データ記録再生装置がディスク状記録媒体を初期化する際の一連の工程を説明するフローチャートである。

【図５】同データ記録再生装置がディスク状記録媒体に対してユーザデータを記録する際の一連の工程を説明するフローチャートである。

【図６】同データ記録再生装置がディスク状記録媒体に記録されているユーザデータを再生する際の一連の工程を説明するフローチャートである。

【図７】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第１の実施の形態

として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図８】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第２の実施の形態として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図９】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第３の実施の形態として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図１０】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第４の実施の形態として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図１１】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第５の実施の形態として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図１２】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第６の実施の形態として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図１３】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第７の実施の形態として示すデータ記録再生装置における暗号化部の動＊作内容を説明する図である。

【図１４】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第８の実施の形態として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図１５】同データ記録再生装置の他の構成を説明するブロック図である。

【図１６】ＤＶＤのフォーマットを説明する図であって、１ブロック分を示す図である。

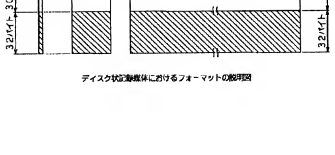
【図１７】ＤＶＤのフォーマットを説明する図であって、ディスク状記録媒体上に並べられるバリティ以外のデータを示す図である。

【図１８】従来のデータ記録再生装置の構成を説明するブロック図である。

【符号の説明】

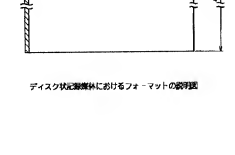
１０　データ記録再生装置、　１１　スピンドルモータ、　１２　光学ピックアップ、　１３　レーザドライバ、　１４　信号検出部、　１５　変復調部、１６　バッファメモリ、　１７　調停部、　１８　ＥＣＣ部、　１９　暗号化部、　２０　入出力部、　２１，２２　レジスタ、　３０　ディスク状記録媒体、ｒ（），ｒ’（）　ランダムデータ発生部、　ｄ（），ｄ’（）　鍵情報分割部、　ｆ（），ｆ’（）　鍵情報生成部、　ｂ（），ｂ’（），ｇ（），ｇ’（），ｅ（），ｅ’（）　暗号化／復号化部

【図１】



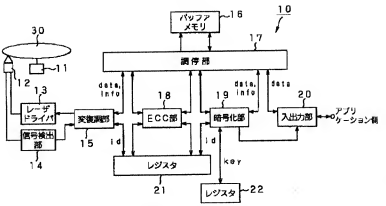
ディスク状記録媒体におけるフォーマットの説明図

【図２】



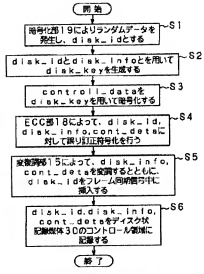
ディスク状記録媒体におけるフォーマットの説明図

【図３】



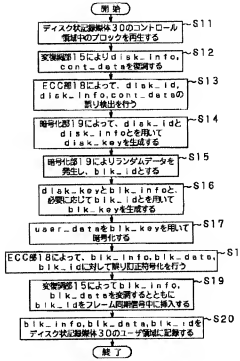
データ記録再生装置の構成ブロック図

【図４】



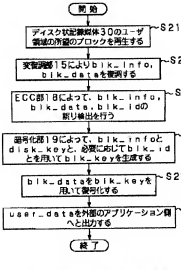
データ記録再生装置における一連の処理工程

【図５】



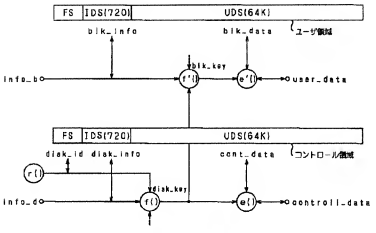
データ記録再生装置における一連の処理工程

【図６】



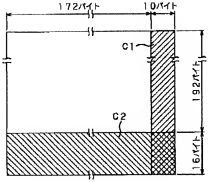
データ記録再生装置における一連の処理工程

【図７】



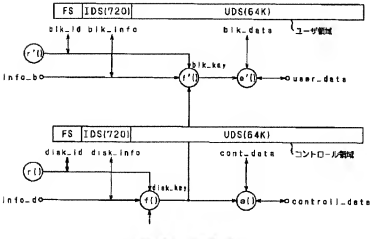
暗号化部の動作内容の説明図

【図１６】



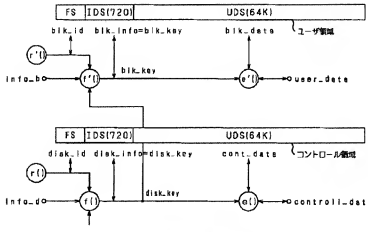
DVDフォーマットの説明図

【図８】



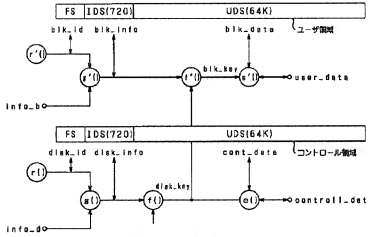
暗号化部の動作内容の説明図

【図９】



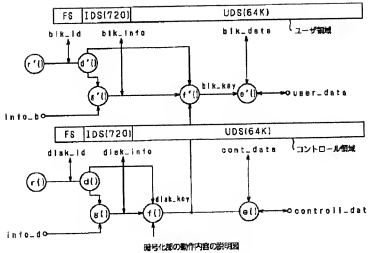
暗号化部の動作内容の説明図

【図１０】



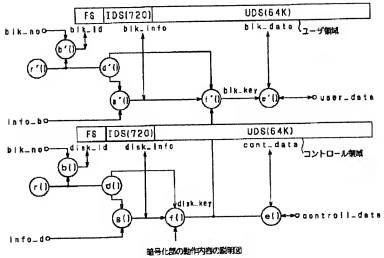
暗号化部の動作内容の説明図

【図１１】



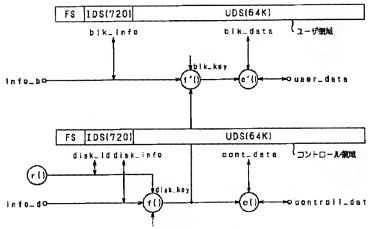
暗号化部の動作内容の説明図

【図１２】



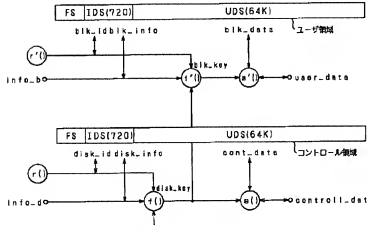
暗号化部の動作内容の説明図

【図１３】



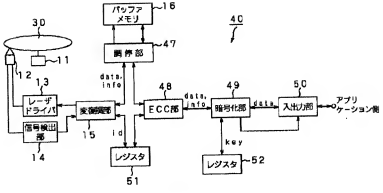
暗号化部の動作内容の説明図

【図１４】



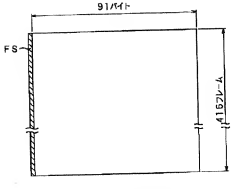
暗号化部の動作内容の説明図

【図１５】



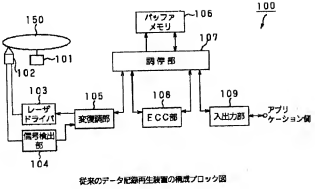
データ記録再生装置の構成ブロック図

【図１７】



DVDフォーマットの説明図

【図１８】



従来のデータ記録再生装置の構成ブロック図